Invariance of Conjunctions of Polynomial Equalities for Algebraic Differential Equations

Khalil Ghorbal[1] **Andrew Sogokon**[2]
André Platzer[1]

July 2014
CMU-CS-14-122

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA, 15213

To appear [15] in the Proceedings of the
21st International Static Analysis Symposium (SAS 2014),
11-13 September 2014, Munich, Germany.

[1] Carnegie Mellon University, Computer Science Department, Pittsburgh, PA, USA
{kghorbal|aplatzer}@cs.cmu.edu
[2] University of Edinburgh, LFCS, School of Informatics, Edinburgh, Scotland, UK
a.sogokon@sms.ed.ac.uk

This material is based upon work supported by the National Science Foundation by NSF CAREER Award CNS-1054246, NSF EXPEDITION CNS-0926181, CNS-0931985, DARPA FA8750-12-2-0291 and EPSRC EP/I010335/1. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of any sponsoring institution or government.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Invariance of Conjunctions of Polynomial Equalities for Algebraic Differential Equations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,School of Computer Science,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In this paper we seek to provide greater automation for formal deductive verification tools working with continuous and hybrid dynamical systems. We present an efficient procedure to check invariance of conjunctions of polynomial equalities under the flow of polynomial ordinary differential equations. The procedure is based on a necessary and sufficient condition that characterizes invariant conjunctions of polynomial equalities. We contrast this approach to an alternative one which combines fast and sufficient (but not necessary) conditions using differential cuts for soundly restricting the system evolution domain.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**37**	

Keywords: algebraic invariant, high-order Lie derivation, differential equation, automated checking, proof rules, continuous dynamics, formal verification

Abstract

In this paper we seek to provide greater automation for formal deductive verification tools working with continuous and hybrid dynamical systems. We present an efficient procedure to check invariance of conjunctions of polynomial equalities under the flow of polynomial ordinary differential equations. The procedure is based on a necessary and sufficient condition that characterizes invariant conjunctions of polynomial equalities. We contrast this approach to an alternative one which combines fast and sufficient (but not necessary) conditions using differential cuts for soundly restricting the system evolution domain.

1 Introduction

The problem of reasoning about invariant sets of dynamical systems is of fundamental importance to verification and modern control design [3, 27, 35, 31]. A set is an invariant of a dynamical system if no trajectory can escape from it. Of particular interest are safety assertions that describe states of the system which are deemed safe; it is clearly important to ensure that these sets are indeed invariant.

Hybrid systems combine discrete and continuous behavior and have found application in modelling a vast quantity of industrially relevant designs, many of which are safety-critical. In order to verify safety properties in hybrid models, one often requires the means of reasoning about safety in continuous systems. This paper focuses on developing and improving the automation of reasoning principles for a particular class of invariant assertions for continuous systems – conjunctions of polynomial equalities; these can be used, e.g. to assert the property that certain values (temperature, pressure, water level, etc.) in the system are maintained at a constant level as the system evolves.

In practice, it is highly desirable to have the means of deciding whether a given set is invariant in a particular dynamical system. It is equally important that such methods be efficient enough to be of practical utility. This paper seeks to address both of these issues. The contributions of this paper are twofold:

- It extends differential radical invariants [14] to obtain a characterization of invariance for algebraic sets under the flow of algebraic differential equations. It also introduces an optimized decision procedure to decide the invariance of algebraic sets.

- It explores an approach combining deductively less powerful rules [19, 33, 22, 30] using differential cuts [28] to exploit the structure of the system to yield efficient proofs even for non-polynomial systems. Furthermore, differential cuts [28] are shown to fundamentally improve the deductive power of Lie's criterion [19].

The two approaches to proving invariance of conjunctive equational assertions explored in this paper are complementary and aim at improving proof automation—deductive power and efficiency—in deductive formal verification tools.

Content. In Section 2, we recall some basic definitions and concepts. Section 3 introduces a new proof rule to check the invariance of a conjunction of polynomial equations along with an optimized implementation. Section 4 presents another novel approach to check invariance of a conjunction; it leverages efficient existing proof rules together with *differential cuts* and *differential weakening*. An automated proof strategy that builds on top of this idea is given in Section 5. The average performance of these different approaches is assessed using a set of 32 benchmarks (Section 6).

2 Preliminaries

Let $\boldsymbol{x} = (x_1, \ldots, x_n) : \mathbb{R}^n$, and $\boldsymbol{x}(t) = (x_1(t), \ldots, x_n(t))$, where $x_i : \mathbb{R} \to \mathbb{R}$, $t \mapsto x_i(t)$. The ring of polynomials over the reals will be denoted by $\mathbb{R}[x_1, \ldots, x_n]$. We consider autonomous[1] differential equations described by polynomial vector fields.

Definition 1 (Polynomial Vector Field)**.** *Let p_i, $1 \leq i \leq n$, be multivariate polynomials in the polynomial ring $\mathbb{R}[\boldsymbol{x}]$. A* polynomial vector field*, $\boldsymbol{p}$, is an explicit system of ordinary differential equations with polynomial right-hand side:*

$$\frac{dx_i}{dt} = \dot{x}_i = p_i(\boldsymbol{x}), \quad 1 \leq i \leq n \ . \tag{1}$$

One important problem is that of checking the invariance of a *variety* (or algebraic set), with evolution domain constraints H; that is, we ask whether a polynomial conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, initially true, holds true in all reachable states[2] that satisfy the evolution domain constraints. The problem is equivalent to the validity of the following formula in differential dynamic logic [27]:

$$(h_1 = 0 \wedge \cdots \wedge h_r = 0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&\, H](h_1 = 0 \wedge \cdots \wedge h_r = 0) \tag{2}$$

where $[\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&\, H]\psi$ is true in a state $\boldsymbol{x}_\iota$ if the postcondition ψ is true in all states reachable from $\boldsymbol{x}_\iota$—satisfying H—by following the differential equation $\dot{\boldsymbol{x}} = \boldsymbol{p}$ for any amount of time as long as H is not violated. For simplicity, for a polynomial h in $\boldsymbol{x}$, we write $h = 0$ for $h(\boldsymbol{x}) = 0$.

Geometrically, the dL formula in Eq. (2) is true if and only if the solution $\boldsymbol{x}(t)$, $t \geq 0$, of the initial value problem ($\dot{\boldsymbol{x}} = \boldsymbol{p}$, $\boldsymbol{x}(0) = \boldsymbol{x}_\iota$), with $h_i(\boldsymbol{x}_\iota) = 0$ for $i = 1, \ldots, r$, is a real root of the system $h_1 = 0, \ldots, h_r = 0$ as long as it satisfies the constraints H.

The algebraic counterpart of varieties are ideals. Ideals are sets of polynomials that are closed under addition and external multiplication. That is, if I is an ideal, then for all $h_1, h_2 \in I$, the sum $h_1 + h_2 \in I$; and if $h \in I$, then, $qh \in I$, for all $q \in \mathbb{R}[x_1 \ldots, x_n]$.

We will use ∇h to denote the gradient of a polynomial h, that is the vector of its partial derivatives $\left(\frac{\partial h}{\partial x_1}, \ldots, \frac{\partial h}{\partial x_n}\right)$. The *Lie derivative* of a polynomial h along a vector field $\boldsymbol{p}$ is defined as follows (the symbol "$\cdot$" denotes the scalar product):

$$\mathfrak{L}_{\boldsymbol{p}}(h) \stackrel{\text{def}}{=} \nabla h \cdot \boldsymbol{p} = \sum_{i=1}^{n} \frac{\partial h}{\partial x_i} p_i \ . \tag{3}$$

Higher-order Lie derivatives are: $\mathfrak{L}_{\boldsymbol{p}}^{(k+1)}(h) = \mathfrak{L}_{\boldsymbol{p}}(\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h))$, where $\mathfrak{L}_{\boldsymbol{p}}^{(0)}(h) = h$.

[1] Autonomous means that the rate of change of the system over time depends only on the system's state, not on time. Non-autonomous systems with time dependence can be made autonomous by adding a new state variable to account for the progress of time.

[2] Reachable states implicitly means that we focus on positive time invariance, that is the time variable t is assumed to be non-negative.

3 Characterizing Invariance of Conjunctive Equations

In this section we give an exact characterization of invariance for conjunctions of polynomial equalities under the flow of algebraic differential equations and assuming that the evolution domain constraint H is an *open* set.[3] The characterization, as well as the proof rule, generalize our previous work which handles purely equational invariants of the form $h = 0$ without considering evolution domains (that is $H = \mathbb{R}^n$, which is open).

The differential radical invariants proof rule DRI [14, Theorem 2] has been shown to be a necessary and sufficient criterion for the invariance of equations of the form $h = 0$:

$$(\mathrm{DRI})\frac{h = 0 \to \bigwedge_{i=0}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0}{h = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\ h = 0}\ . \tag{4}$$

The *order* $N \geq 1$ denotes the length of the chain of ideals $\langle h\rangle \subseteq \langle h, \mathfrak{L}_{\boldsymbol{p}}(h)\rangle \subseteq \cdots$ which reaches a fixed point after finitely many steps by the ascending chain property of Noetherian rings. Thus, the order N is always finite and computable—using Göbner Bases [5]—for polynomials with rational coefficients. The premise of the proof rule DRI is a real quantifier elimination problem and can be solved algorithmically [6].

A naïve approach to prove invariance of a conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, without evolution domain constraints, is to use the proof rule DRI together with the following sum-of-squares equivalence from real arithmetic:

$$h_1 = 0 \wedge \cdots \wedge h_r = 0\ \equiv_{\mathbb{R}}\ \sum_{i=1}^{r} h_i^2 = 0\ . \tag{5}$$

Sums-of-squares come at the price of doubling the polynomial degree, thereby increasing the complexity of checking the premise (Section 3.2 discusses the link between polynomial degree and the complexity of DRI-based proof rules). Instead, we present an extension of the proof rule DRI that exploits the underlying logical structure of conjunctions. For a conjunction of equations $h_1 = 0 \wedge \cdots \wedge h_r = 0$, the order N is generalized to the length of the chain of ideals formed by *all* the polynomials $h_1, \ldots, h_r$ and their successive Lie derivatives:

$$I = \langle h_1, \ldots, h_r\rangle \subseteq \langle h_1, \ldots, h_r, \mathfrak{L}_{\boldsymbol{p}}(h_1), \ldots, \mathfrak{L}_{\boldsymbol{p}}(h_r)\rangle \subseteq \langle h_1, \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h_r)\rangle \cdots \tag{6}$$

Theorem 1 (Conjunctive Differential Radical Characterization)**.** *Let $h_1, \ldots, h_r \in \mathbb{R}[\boldsymbol{x}]$ and let H denote some* open *evolution domain constraint. Then, the conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, is invariant under the flow of the vector field $\boldsymbol{p}$, subject to the evolution constraint H, if and only if*

$$H \vdash \bigwedge_{j=1}^{r} h_j = 0 \to \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j) = 0\ . \tag{7}$$

where N denotes the order of the conjunction.

[3] We will briefly discuss the case when H is an arbitrary set later. We leave the formal treatment of the general case as a future work.

Here $\vdash$ is used, as in sequent calculus, to assert that whenever the constraint H (antecedent) is satisfied, then at least one (in this case, the only) formula to the right of $\vdash$ is also true. The detailed proof can be found Appendix A. When the evolution domain constraints are dropped ($H = \text{True}$) and $r = 1$ (one equation), one recovers exactly the statement of [14, Theorem 2] which characterizes invariance of atomic equations. Intuitively, Theorem 3 says that on the invariant algebraic set, all higher-order Lie derivatives of each polynomial h_i must vanish. It adds however a crucial detail: checking finitely many—exactly N—higher-order Lie derivatives is both necessary and sufficient. The theorem does not check for invariance of each conjunct taken separately, rather it handles the conjunction simultaneously. The order N is a property of the ideal chain formed by *all* the polynomials and their Lie derivatives. If N_i denotes the order of each atom h_i taken separately, then one can readily see that

$$N \leq \max_i N_i \ . \tag{8}$$

The equality does not hold in general: consider for instance $h_1 = x_1$, $h_2 = x_2$ and $\boldsymbol{p} = (x_2, x_1)$. Since $\mathfrak{L}^{(2)}_{\boldsymbol{p}}(h_i) = h_i$, for $i = 1, 2$, we have $N_1 = N_2 = 2$. However,

$$\langle x_1, x_2\rangle = \langle h_1, h_2\rangle \subseteq \langle h_1, h_2, \mathfrak{L}_{\boldsymbol{p}}(h_1), \mathfrak{L}_{\boldsymbol{p}}(h_2)\rangle = \langle x_1, x_2, x_2, x_1\rangle = \langle x_1, x_2\rangle,$$

which means that $N = 1$. This example highlights one of the main differences between this work and the characterization given in [21, Theorem 24], where the criterion is given by

$$H \vdash \bigwedge_{j=1}^{r} h_j = 0 \rightarrow \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N_j - 1} \mathfrak{L}^{(i)}_{\boldsymbol{p}}(h_j) = 0 \ . \tag{9}$$

The computation of *each* order N_j requires solving N_j ideal membership problems. One can appreciate the difference with the criterion of Theorem 3 which only requires N ideal membership checks for the entire conjunction. In the worst case, when $N = N_k = \max_i N_i$, Theorem 3 performs $\sum_{j=1, j\neq k}^{r} N_j$ fewer ideal membership checks compared to the criterion of Eq. (9). A smaller order N confers an additional benefit of reducing the cost of quantifier elimination—discussed in Section 3.2—by bringing down both the total number of polynomials and their maximum degree.

Remark 1 (Reducing the Differential Radical Order Using the Evolution Domain Constraint)**.** *Ideally, one should also account for H when computing N. When H is an algebraic set, its generators should be appended to the ideal $\langle h_1, \ldots, h_r\rangle$. We leave the semi-algebraic case for future work. For instance, consider the vector field $\boldsymbol{p} = (x_2 - 1, x_1 - 2)$ and the candidate $h = x_2 - 1$ subject to $H : x_1 - 2 = 0$. The differential radical order of $\langle x_2 - 1\rangle$ is 2. If we consider H, the ideal to consider would be $\langle x_1 - 2, x_2 - 1\rangle$ leading to $N = 1$.*

Using Theorem 3, the differential radical invariant proof rule DRI [14] generalizes to conjunctions of equations with evolution domain constraints as follows:

$$(\mathrm{DRI}_\wedge)\frac{H \vdash \left(\bigwedge_{j=1}^{r} h_j = 0\right) \rightarrow \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N-1} \mathfrak{L}^{(i)}_{\boldsymbol{p}}(h_j) = 0}{\left(\bigwedge_{j=1}^{r} h_j = 0\right) \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&\, H] \left(\bigwedge_{j=1}^{r} h_j = 0\right)} \ . \tag{10}$$

Next, we implement the proof rule $\mathrm{DRI}_\wedge$ and discuss its theoretical complexity.

Algorithm 1: Checking invariance of a conjunction of polynomial equations.

Data: H (evolution domain constraints), $\boldsymbol{p}$ (vector field), $\boldsymbol{x}$ (state variables)
Data: $h_1, \ldots, h_r$ (conjunction candidate)
Result: True if and only if $h_1 = 0 \wedge \ldots \wedge h_r = 0$ is an invariant of $[\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&\, H]$

1 $\check{N} \leftarrow 1$
2 $\mathtt{I} \leftarrow \{h_1, \ldots, h_r\}$ `// Elements of the chain of ideals`
3 $\mathtt{L} \leftarrow \{h_1, \ldots, h_r\}$ `// Work list of polynomial to derive`
4 `symbs` $\leftarrow$ Variables[$\boldsymbol{p}, h_1, \ldots, h_r$]
5 **while** True **do**
6 `GB` $\leftarrow$ GröbnerBasis[`I`, $\boldsymbol{x}$]
7 `LD` $\leftarrow \{\}$ `// Work list of Lie derivatives not in I`
8 **foreach** ℓ in `L` **do**
9 `LieD` $\leftarrow$ LieDerivative[ℓ, $\boldsymbol{p}$, $\boldsymbol{x}$]
10 `Rem` $\leftarrow$ PolynomialRemainder[`LieD`, `GB`, $\boldsymbol{x}$]
11 **if** `Rem` $\neq 0$ **then**
12 `LD` $\leftarrow$ `LD` $\cup$ `LieD`
13 **if** `LD` $= \{\}$ **then**
14 **return** True
15 **else**
16 **foreach** ℓ in `LD` **do**
17 **if** QE[$\forall$ `symbs` $(H \wedge h_1 = 0 \wedge \cdots \wedge h_r = 0 \rightarrow \ell = 0)$] $\neq$ True **then**
18 **return** False
19 `I` $\leftarrow$ `GB` $\cup$ `LD`
20 $\check{N} \leftarrow \check{N} + 1$
21 `L` $\leftarrow$ `LD`

3.1 Decision Procedure

To check the validity of the premise in the proof rule $\mathrm{DRI}_\wedge$, one needs to compute the order N and to decide a purely universally quantified sentence in the theory of real arithmetic. These two tasks do not have to be performed in that precise order. We present an algorithm that computes N on the fly while breaking down the quantifier elimination problem into simpler sub-problems.

Algorithm 1 implements the proof rule $\mathrm{DRI}_\wedge$. The algorithm returns True if and only if the candidate is an invariant. The variable $\check{N}$ strictly increases and converges, from below, toward the finite unknown order N. It is therefore a decision procedure for the invariance problem with conjunctive equational candidates.

At each iteration of the **while** loop it checks whether a fixed point of the chain of ideals has been reached, implying $\check{N} = N$. To this end, it computes a Gröbner basis (`GB`) of the ideal `I` (line 2), containing the polynomials h_i as well as their respective higher-order Lie derivatives up to the

derivation order $\check{N}-1$. Then it enters a **foreach** loop (line 8), where it computes the $\check{N}$th order Lie derivatives and their respective reductions (or remainders) (`LieD`) by the Gröbner basis `GB`. All Lie derivatives with non-zero remainders are stored in the list `LD` (line 12). If the list is empty, then all $\check{N}$th Lie derivatives are in the ideal `I`: the fixed point of the chain of ideals is reached, and $\check{N}=N$. This also means that True can be returned since all prior quantifier elimination calls returned True. Otherwise, the outermost **while** loop (line 5) needs to be executed one more time after increasing $\check{N}$ (line 20). Before re-executing the **while** loop, however, we make sure that the premise of the proof rule $\mathrm{DRI}_\wedge$ holds up to $\check{N}$. Since in this case, we know that $\check{N}<N$, if the quantifier elimination fails to discharge the premise of the proof rule $\mathrm{DRI}_\wedge$ at $\check{N}$, then we do not need to go any further as the invariance property is already falsified.

The **while** loop decomposes the right hand side of the implication in Eq. (10) along the conjunction $\bigwedge_{i=1}^{N-1}$: the ith iteration checks whether the conjunction $\bigwedge_{j=1}^{r}\mathfrak{L}_{\boldsymbol{p}}^{(i)}h_j$ vanishes. The main purpose of the **foreach** loop in line 16 is to decompose further the conjunction $\bigwedge_{j=1}^{r}$ using the logical equivalence $a\rightarrow(b\wedge c)\equiv(a\rightarrow b)\wedge(a\rightarrow c)$ for any boolean variables a, b, and c. This leads to more tractable problems of the form:

$$H\vdash\bigwedge_{j=1}^{r}h_j=0\rightarrow\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j)=0\ . \tag{11}$$

Observe that the quantifier elimination problem in line 17 performs a universal closure for all involved symbols—state variables and parameters— denoted by `symbs` and determined once at the beginning of the algorithm using the procedure `Variables` (line 4). Besides, the quantifier elimination problem in line 17 can be readily adapted to explicitly return extra conditions on the parameters to ensure invariance of the given conjunction. When the algorithm returns False, any counterexample to the quantifier elimination problem of line 17 can be used as an initial condition for a concrete counterexample that falsifies the invariant.

3.2 Complexity

Algorithm 1 relies on two expensive procedures: deciding purely universally quantified sentences in the theory of real arithmetic (line 17) and ideal membership of multivariate polynomials using Gröbner bases (line 6). We discuss their respective complexity.

Quantifier elimination over the reals is decidable [36]. The purely existential fragment of the theory of real arithmetic has been shown to exhibit singly exponential time complexity in the number of variables [1]. Theoretically, the best bound on the complexity of deciding a sentence in the existential theory of $\mathbb{R}$ is given by $(sd)^{O(n)}$, where s is the number of polynomials in the formula, d their maximum degree and n the number of variables [1]. However, in practice this has not yet led to an efficient decision procedure, so typically it is much more efficient to use partial cylindrical algebraic decomposition (PCAD) due to Collins & Hong [6], which has running time complexity doubly-exponential in the number of variables.

Ideal membership of multivariate polynomials with rational coefficients is complete for `EXPSPACE` [23]. Gröbner bases [5] allow membership checks in ideals generated by multivariate polynomials. Significant advances have been made for computing Gröbner bases [11, 12] which in practice can

be expected to perform very well. The degree of the polynomials involved in a Gröbner basis computation can be very large. Theoretically, a Gröbner basis may contain polynomials with degree 2^{2^d} [24]. The degrees of all the polynomials involved are bounded by $O(d^{2^n})$ [10]. Gröbner bases are also highly sensitive to the monomial order arranging the different monomials of a multivariate polynomial (see, e.g., [8, Chapter 2] for formal definitions). The Degree Reverse Lexicographic (`degrevlex`) order gives (on average) Gröbner bases with the smallest total degree [2], although there exist known examples (cf. Mora's example in [18]) for which, even for the `degrevlex` monomial ordering, the (reduced) Gröbner basis contains a polynomial of total degree $O(d^2)$. Finally, the rational coefficients of the generators of Gröbner bases may become involved (compared to the rational coefficients of the original generators of the ideal), which can have a negative impact on the running time and memory requirements.

3.3 Optimization

The theoretical complexity of both the quantifier elimination and Gröbner bases algorithms suggests several opportunities for optimization for Algorithm 1. The maximal degree of the polynomials appearing in H is assumed to be fixed. We can reduce the polynomial degrees in the right-hand side of the implication in Eq. (11) as follows: by choosing a total degree monomial ordering (e.g. `degrevlex`), the remainder `Rem` has at most the same total degree as `LieD`; replacing `LieD` by `Rem` serves to reduce (on average) the cost of calling a quantifier elimination procedure. Lem. 1 proves that substituting `LieD` by its remainder `Rem` in line 17 does not compromise correctness.

Lemma 1. *Let q be the remainder of the reduction of the polynomial s by the Gröbner basis of the ideal generated by the polynomials $h_1, \ldots, h_r$. Then,*

$$h_1 = 0 \wedge \cdots \wedge h_r = 0 \rightarrow s = 0 \textit{ if and only if } h_1 = 0 \wedge \cdots \wedge h_r = 0 \rightarrow q = 0 \ .$$

Proof. By construction, we have $s = \sum_{i=1}^{r} \alpha_i h_i + q$ for some polynomials α_i. Therefore, the conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$ implies that $s - q = 0$, or equivalently $s = q$, and the lemma follows. □

The same substitution reduces the Gröbner basis computation cost since it attempts to keep a low maximal degree in all the polynomials appearing in the generators of the ideal `I`. Lem. 2 shows that it is safe to perform this substitution: the ideal `I` remains unchanged regardless of whether we choose to construct the list `LD` using `LieD` or `Rem`.

Lemma 2. *Let q be the remainder of the reduction of the polynomial s by the Gröbner basis of the ideal generated by the polynomials $h_1, \ldots, h_r$. Then,*

$$\langle h_1, \ldots, h_r, s \rangle = \langle h_1, \ldots, h_r, q \rangle \ .$$

Proof. By construction, we have $s = \sum_{i=1}^{r} \alpha_i h_i + q$ for some polynomials α_i. Therefore, $s \in \langle h_1, \ldots, h_r, q \rangle$ and $q \in \langle h_1, \ldots, h_r, s \rangle$, which respectively leads to
$\langle h_1, \ldots, h_r, s \rangle \subseteq \langle h_1, \ldots, h_r, q \rangle$ and $\langle h_1, \ldots, h_r, s \rangle \supseteq \langle h_1, \ldots, h_r, q \rangle$. □

$$(\mathrm{DI}_{=})\frac{H \vdash \mathfrak{L}_{\boldsymbol{p}}(h) = 0}{(h=0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ H](h=0)} \qquad (\text{P-c})\frac{H \vdash \mathfrak{L}_{\boldsymbol{p}}(h) \in \langle h \rangle}{(h=0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ H](h=0)}$$

$$(\mathrm{Lie})\frac{\bigwedge_{i=1}^{k-1} g_i = 0 \vdash h = 0 \to (\mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathrm{rank}(\nabla g_1, \ldots, \nabla g_{k-1}, \nabla h) = k)}{(h=0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ \bigwedge_{i=1}^{k-1} g_i = 0](h=0)}$$

$$(\mathrm{Lie}_o)\frac{H \vdash h = 0 \to (\mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \nabla h \neq \mathbf{0})}{(h=0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ H](h=0)} \qquad (\mathrm{DW})\frac{H \vdash F}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&H\ ]F}$$

Figure 1: Proof rules for checking the invariance of $h = 0$ w.r.t. the vector field $\boldsymbol{p}$: $\mathrm{DI}_{=}$ [30, Theorem 3], P-c [33, Lemma 2], Lie, Lie_o based on [26, Theorem 2.8], DW [29, Lemma 3.6]

Although this optimization reduces the total degree of the polynomials involved, the coefficients of the remainder q may get more involved than the coefficients of the original polynomial s. In Section 6 we give an empirical comparison of the optimized—as detailed in this section—versus the unoptimized version of Algorithm 1.

4 Sufficient Conditions for Invariance of Equations

The previous section dealt with a method for proving invariance which is both necessary and sufficient for conjunctions of polynomial equalities. Given the proof rule $\mathrm{DRI}_{\wedge}$, it is natural to ask whether previously proposed *sufficient* proof rules are still relevant. After all, theoretically, $\mathrm{DRI}_{\wedge}$ is all that is required for producing proofs of invariance in this class of problems. This is a perfectly legitimate question; however, given the complexity of the underlying decision procedures needed for $\mathrm{DRI}_{\wedge}$ it is perhaps not surprising that one will eventually face scalability issues. This, in turn, motivates a different question - can one use proof rules (which are perhaps deductively weaker than $\mathrm{DRI}_{\wedge}$) in such a way as to attain more computationally efficient proofs of invariance?

Before addressing this question, this section will review existing sufficient proof rules which allow reasoning about invariance of atomic equational assertions. In Fig. 1, $\mathrm{DI}_{=}$ shows the equational differential invariant [28] proof rule. The condition is sufficient (but not necessary) and characterizes polynomial invariant functions [28, 30]. The premise of the Polynomial-consecution rule [33, 22], P-c in Fig. 1, requires $\mathfrak{L}_{\boldsymbol{p}}(h)$ to be in the ideal generated by h. This condition is also only sufficient and was mentioned as early as 1878 [9]. The Lie proof rule uses Lie's criterion [19, 26, 30] for invariance of $h = 0$ and characterizes *smooth* invariant manifolds, while Lie_o is a common variant that assumes the evolution constraint H provided that it defines an open set.

Remark 2. *In an earlier version,* Lie_o *was incorrectly represented as* Lie*, which only applies to instances where* H *is open. See [26, 30] for more information about Lie's criterion.*

The rule DW is called *differential weakening* [29] and covers the trivial case when the evolution constraint implies the invariant candidate; in contrast to all other rules in the table, DW can work with arbitrary invariant assertions.

Unlike the necessary and sufficient condition provided by the rule DRI (see Eq. (4)), all the other proof rules in Figure 1 only impose sufficient conditions and may thus fail at a proof even in cases when the candidate is indeed an invariant.

The purpose of all the rules shown in Figure 1, save perhaps DW, is to show invariance of atomic equations. However, in general, one faces the problem $F \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&\, H]C$, where F is a formula defining a set of states where the system is initialized, and C is the post-condition where the system always enters after following the differential equation $\dot{\boldsymbol{x}} = \boldsymbol{p}$ as long as the domain constraint H is satisfied.

One way to prove such a statement is to find an invariant I which is true initially (i.e. $F \to I$), is indeed an invariant for the system ($I \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&\, H]I$), and implies the post-condition ($I \to C$). These conditions can be formalized in the proof rule [31]

$$(\mathrm{Inv})\frac{F \to I \qquad I \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]I \qquad I \to C}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]C}.$$

In this paper we consider the special case when the invariant is the same as the post-condition, so we can drop the last clause and the rule becomes

$$(\mathrm{Inv})\frac{F \to C \qquad C \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]C}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]C}.$$

In the following sections, we will be working in a proof calculus, rather than considering a single proof rule, and will call upon this definition in the proofs we construct.

5 Differential Cuts and Lie's Rule

When considering a conjunctive invariant candidate $h_1 = 0 \wedge h_2 = 0 \wedge \cdots \wedge h_r = 0$, it may be the case that each conjunct considered separately is an invariant for the system. Then, one could simply invoke the following basic result about invariant sets to prove invariance of each atomic formula individually.

Proposition 1. *Let $S_1, S_2 \subseteq \mathbb{R}^n$ be invariant sets for the differential equation $\dot{\boldsymbol{x}} = \boldsymbol{p}$, then the set $S_1 \cap S_2$ is also an invariant.*

Corollary 1. *The proof rule*

$$(\wedge_{\mathrm{Inv}})\frac{h_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]h_1 = 0 \qquad h_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]h_2 = 0}{h_1 = 0 \wedge h_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,](h_1 = 0 \wedge h_2 = 0)} \tag{12}$$

is sound and may be generalized to accommodate arbitrarily many conjuncts.

Of course, one still needs to choose an appropriate proof rule from Figure 1 (or DRI) in order to prove invariance of atomic equational formulas. For purely polynomial problems it would be natural to attempt a proof using DRI first, but in the presence of transcendental functions, one may need to resort to other rules. In general however, even if the conjunction defines an invariant set,

the individual conjuncts need *not* themselves be invariants. If such is the case, one cannot simply break down the conjunctive assertion using the rule $\wedge_{\mathrm{Inv}}$ and prove invariance of each conjunct individually. In this section, we explore using a proof rule called *differential cut* (DC) to address this issue.

Differential cuts were introduced as a fundamental proof principle for differential equations [28] and can be used to (soundly) strengthen assumptions about the system evolution.

Proposition 2 (Differential Cut [28])**.** *The proof rule*

$$(\mathrm{DC})\frac{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]C \qquad F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ C]F}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]F},$$

where C and F denote quantifier-free first-order formulas, is sound.

Remark 3. *The rule $\wedge_{\mathrm{Inv}}$ may in fact be derived from* DW*,* Inv*, and* DC*.*

One may appreciate the geometric intuition behind the rule DC if one realizes that the left branch requires one to show that the set of states satisfying C is an invariant for the system initialized in any state satisfying F. Thus, the system does not admit any trajectories starting in F that leave C and hence by adding C to the evolution constraint, one does not restrict the behavior of the original system.

Differential cuts may be applied repeatedly to the effect of refining the evolution constraint with more invariant sets. It may be profitable to think of successive differential cuts as showing an *embedding of invariants* in a system.

There is an interesting connection between differential cuts and embeddings of invariant sub-manifolds, when used with the proof rule Lie. To develop this idea, let us remark that if one succeeds at proving invariance of some $h_1 = 0$ using the rule Lie in a system with no evolution constraint, one shows that $h_1 = 0$ is a smooth invariant sub-manifold of $\mathbb{R}^n$. If one now considers the system evolving inside that invariant manifold and finds some $h_2 = 0$ which can be proved to be invariant using Lie with $h_1 = 0$ acting as an evolution constraint, then inside the manifold $h_1 = 0$, $h_2 = 0$ defines an invariant sub-manifold (even in cases when $h_2 = 0$ might not define a sub-manifold of the ambient space $\mathbb{R}^n$). One can proceed using Lie in this way to look for further embedded invariant sub-manifolds. We will illustrate this idea using a basic example.

Example 1 (Differential cut with Lie)**.** *Let the system dynamics be $\boldsymbol{p} = (x_1, -x_2)$. This system has an equilibrium at the origin, i.e. $\boldsymbol{p}(\mathbf{0}) = \mathbf{0}$. Consider an invariant candidate $x_1 = 0 \wedge x_1 - x_2 = 0$. One cannot use* Lie *directly to prove the goal*

$$x_1 = 0 \wedge x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\ (x_1 = 0 \wedge x_1 - x_2 = 0)\ .$$

Indeed, rewriting $x_1 = 0 \wedge x_1 - x_2 = 0$ as $x_1^2 + (x_1 - x_2)^2 = 0$ and attempting to use Lie *will not succeed as $h = 0 \to \nabla(x_1^2 + (x_1 - x_2)^2) = 0$.*

Instead, DC *can be used to cut by $x_1 = 0$, which is an invariant for this system provable using* Lie*. The left branch of* DC *is proved as follows:*

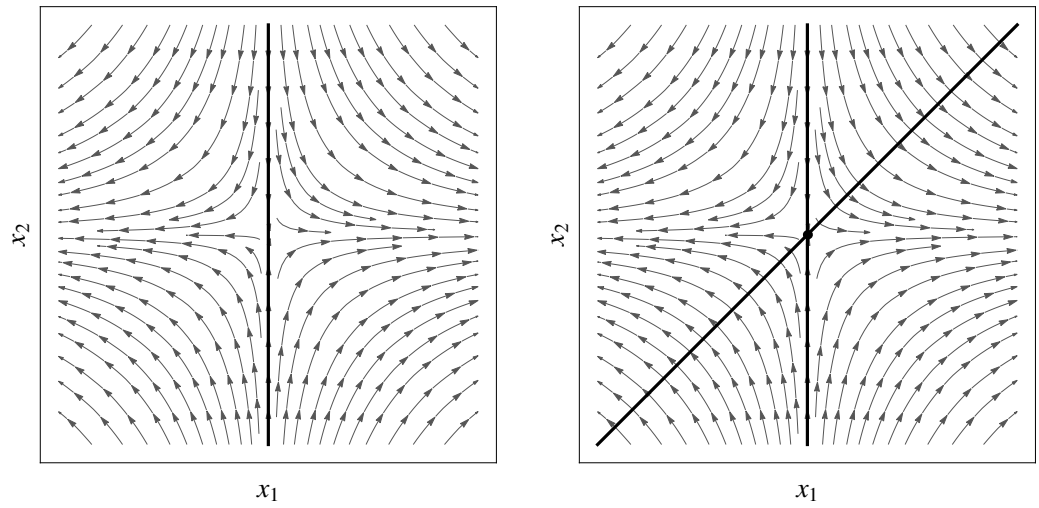

Figure 2: System invariant $x_1 = 0$ (**left**) used in a differential cut to show that the intersection at the origin (**right**) is an invariant.

$$\dfrac{\dfrac{*}{x_1 = 0 \land x_1 - x_2 = 0 \to x_1 = 0}\,(\mathbb{R}) \qquad \dfrac{\dfrac{*}{x_1 = 0 \to x_1 = 0 \land (1 \neq 0)}\,(\mathbb{R})}{x_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, x_1 = 0}\,(\text{Lie})}{x_1 = 0 \land x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, x_1 = 0}\,(\text{Inv})$$

One can also prove that $x_1 - x_2 = 0$ *is a invariant under the evolution constraint* $x_1 = 0$*:*

$$\dfrac{\dfrac{*}{x_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, x_1 = 0]\, x_1 = 0}\,(\text{DW}) \qquad \dfrac{\dfrac{*}{x_1 = 0 \vdash x_1 - x_2 = 0 \to x_1 + x_2 = 0 \land \operatorname{rank}(\nabla(x_1), \nabla(x1 - x2)) = 2}\,(\mathbb{R})}{x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, x_1 = 0]\, x_1 - x_2 = 0}\,(\text{Lie})}{x_1 = 0 \land x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, x_1 = 0]\, (x_1 = 0 \land x_1 - x_2 = 0)}\,(\land_{\text{Inv}})$$

Using these two sub-proofs to close the appropriate branches, the rule DC *proves*

$$x_1 = 0 \land x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,]\, (x_1 = 0 \land x_1 - x_2 = 0).$$

While this example is very simplistic, it provides a good illustration of the method behind differential cuts. We used DC *to restrict system evolution to an invariant manifold* $x_1 = 0$ *using* Lie *and then used* Lie *again to show that* $x_1 - x_2 = 0$ *defines an invariant sub-manifold inside* $x_1 = 0$*. This is illustrated in Fig. 2.*

It is also worth noting that the choice of conjunct for use in the differential cut was crucial. Had we initially picked $x_1 - x_2 = 0$ *to act as* C *in* DC*, the proof attempt would have failed, since this does not define an invariant sub-manifold of* $\mathbb{R}^2$ *(see Fig. 2).*

Let us now remark that by employing DC, we proved invariance of a conjunction which could not be described by an atomic equational assertion which is provable using the rule Lie, or by using Lie to prove invariance of each conjunct after breaking down the conjunction with the rule $\land_{\text{Inv}}$. It has previously been shown that differential cuts increase the deductive power of the system when used in concert with differential invariants [28, 31, 30]. We prove that the same is true for

differential cuts with Lie. Indeed, differential cuts serve to address some of the limitations inherent in both $\mathrm{DI}_=$ and Lie.

Theorem 2. *The deductive power of* Lie *together with* DC *is strictly greater than that of* Lie *considered separately. We write this as* $\mathrm{DC} + \mathrm{Lie} \succ \mathrm{Lie}$.

Proof. In Example 1 we demonstrate the use of Lie together with DC to prove invariance of a conjunction of polynomial equalities which is *not* provable using Lie alone. To see this, suppose that for the system in Example 1 there exists some real-valued differentiable function $g(\boldsymbol{x})$ whose zero level set is precisely the origin, i.e. $(g(\boldsymbol{x}) = 0) \equiv (\boldsymbol{x} = \mathbf{0})$. Then, for all $\boldsymbol{x} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}$ this function evaluates to $g(\boldsymbol{x}) > 0$ or $g(\boldsymbol{x}) < 0$ (by continuity of $g(\boldsymbol{x})$) and $\mathbf{0}$ is thus the global minimum or global maximum, respectively. In either case, $g(\boldsymbol{x}) = 0 \implies \nabla g(\boldsymbol{x}) = \mathbf{0}$ is valid, which cannot satisfy the premise of Lie. □ □

Similar to the embedding of invariants observed when combining differential cuts with Lie proof rule, we briefly explore an intriguing connection between the use of differential cuts together with $\mathrm{DI}_=$ and *higher integrals* of dynamical systems.

The premise of the rule $\mathrm{DI}_=$ establishes that $h(\boldsymbol{x})$ is a *first integral* (i.e. a constant of motion) for the system in order to conclude that $h = 0$ is an invariant. More general notions of invariance have been introduced to study integrability of dynamical systems. For instance, $h(\boldsymbol{x})$ is a *second integral* if $\mathfrak{L}_{\boldsymbol{p}}(h) = \alpha h$, where α is some function; this is also sufficient to conclude that $h = 0$ is an invariant. Let us remark that in a purely polynomial setting, such an $h \in \mathbb{R}[\boldsymbol{x}]$ is known as a *Darboux polynomial* [16, 9] and the condition corresponds to ideal membership in the premise of P-c. Going further, a *third integral* is a function $h(\boldsymbol{x})$ that remains constant on some level set of a first integral $g(\boldsymbol{x})$ [16, Section 2.6], i.e. $\mathfrak{L}_{\boldsymbol{p}}(h) = \alpha g$ where g is a first integral and α is some function. These ideas generalize to higher integrals (see [16, Section 2.7]).

Example 2 (Deconstructed aircraft [30] - differential cut with $\mathrm{DI}_=$)**.** *Consider the system* $\dot{\boldsymbol{x}} = \boldsymbol{p} = (-x_2, x_3, -x_2)$ *and consider the invariant candidate* $x_1^2 + x_2^2 = 1 \land x_3 = x_1$. *One cannot use* $\mathrm{DI}_=$ *directly to prove the goal*

$$x_1^2 + x_2^2 = 1 \land x_3 = x_1 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\,(x_1^2 + x_2^2 = 1 \land x_3 = x_1)\,.$$

We can apply DC *to cut by* $x_1 = x_3$*, which is a first integral for the system and is thus provable using* $\mathrm{DI}_=$. *The left branch of* DC *is proved as follows:*

$$\dfrac{(\mathrm{Inv})\ \dfrac{(\mathbb{R})\ \dfrac{*}{x_1^2 + x_2^2 = 1 \land x_3 = x_1 \to x_3 = x_1} \qquad (\mathrm{DI}_=)\ \dfrac{(\mathbb{R})\ \dfrac{*}{-x_2 = -x_2}}{x_3 = x_1 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]x_3 = x_1}}{x_1^2 + x_2^2 = 1 \land x_3 = x_1 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]x_3 = x_1}$$

For the right branch of DC *we need to show that* $x_1^2 + x_2^2 = 1$ *is an invariant under the evolution constraint* $x_3 = x_1$. *This is again provable using* $\mathrm{DI}_=$*:*

$$\dfrac{\dfrac{}{x_3 = x_1 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, x_3 = x_1]\, x_3 = x_1}(\mathrm{DW}) \quad \dfrac{\dfrac{}{x_3 = x_1 \vdash -2x_1x_2 + 2x_2x_3 = 0}(\mathbb{R})}{x_1^2 + x_2^2 = 1 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, x_3 = x_1]\, x_1^2 + x_2^2 = 1}(\mathrm{DI}_{=})}{x_1^2 + x_2^2 = 1 \wedge x_3 = x_1 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, x_3 = x_1]\, (x_1^2 + x_2^2 = 1 \wedge x_3 = x_1)}(\wedge_{\mathrm{Inv}})$$

We can now construct a proof of invariance for the conjunction using DC.

Note that in this example, we have only ever had to resort to the rule $\mathrm{DI}_{=}$ *for showing invariance of an equational candidate. We first showed that* $x_3 - x_1$ *is an invariant function (first integral) for the system. After restricting the evolution domain to the zero set of the first integral,* $x_3 - x_1 = 0$*, we proved that the polynomial* $x_1^2 + x_2^2 - 1$ *is conserved in the constrained system. In this example we have* $\mathfrak{L}_{\boldsymbol{p}}(x_1^2 + x_2^2 - 1) = -2x_1x_2 + 2x_2x_3 = 2x_2(x_3 - x_1)$*, where* $(x_3 - x_1)$ *is a first integral of the system. Thus,* $x_1^2 + x_2^2 - 1$ *is in fact a (polynomial) third integral.*

5.1 Proof Strategies using Differential Cuts

Differential cuts can be used to search for a proof of invariance of conjunctive equational assertions. This involves selecting some conjunct $h_i = 0$ to cut by (that is use it as C in DC). If the conjunct is indeed an invariant, it will be possible to strengthen the evolution domain constraint and proceed in a similar fashion by selecting a new C from the remaining conjuncts until a proof is attained. A formal proof of invariance using differential cuts can be quite long and will repeatedly resort to proof rules such as $(\wedge_{\mathrm{Inv}})$ (Eq. (12)) and DW (Fig. 1), which is used to prune away conjuncts that have already been added to the evolution domain constraint.

Algorithm 2: `DCSearch`. Differential cut proof search

Data: $\{h_1, \ldots, h_r\}$, $\boldsymbol{p}$, H
Result: True, False.

```
if r = 0 then
    return True
else
    i ← 1
    while i ≤ r do
        if Inv(h_i, H) then
            if DCSearch({h_1 ..., h_r} \ {h_i}, p, H ∧ h_i = 0) then
                return True
        else
            i ← i + 1
    return False
```

Our proof strategy iteratively selects a conjunct with which to attempt a differential cut as a recursive function DCSearch, shown in Algorithm 2. Before calling this function, the conjuncts are put into ascending order with respect to the number of variables appearing in the conjunct.

For purely polynomial problems, the ordering is also ascending with respect to the total degree of the polynomials. The aim of this pre-processing step is to ensure that conjuncts which are potentially less expensive to check for invariance are processed first (see Section 3.2). There is in general no easy way of selecting the "right" proof rule for showing invariance of atomic equations (step `Inv` line 6 of Algorithm 2); a possible, albeit not very efficient, solution would be to iterate through all the available proof rules. This would combine their deductive power, but could also lead do diminished performance. In practice, selecting a good proof rule for atomic invariants is very much a problem-specific matter. We have implemented $\mathrm{DCSearch}$ to use the proof rule $\mathrm{DI}_{=}$ before trying Lie.

The overall proof strategy, if successful, would lead to a proof tree resembling that shown below. The proof steps labelled with ? mark choices in selecting the rule for atomic invariants from Figure 1.

$$\dfrac{\dfrac{\dfrac{*}{\bigwedge_{i=1}^{r} h_i = 0 \to h_1 = 0}\,(\mathbb{R})}{\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, h_1 = 0}\,(\mathrm{Inv}) \qquad \dfrac{\dfrac{*}{h_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, h_1 = 0}\,?}{\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, h_1 = 0}\,(\mathrm{DC}) \qquad \dfrac{\dfrac{*}{h_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, h_1 = 0]\, h_1 = 0}\,(\mathrm{DW})}{\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, h_1 = 0]\, \bigwedge_{i=1}^{r} h_i = 0}\,(\wedge_{\mathrm{inv}}) \qquad \dfrac{\dfrac{\dfrac{*}{h_r = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, \bigwedge_{i=1}^{r-1} h_i = 0]\, h_r = 0}\,?}{\bigwedge_{i=2}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, h_1 = 0]\, \bigwedge_{i=2}^{r} h_i = 0}\,(\mathrm{DC})}{\vdots}}{\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, h_1 = 0]\, \bigwedge_{i=1}^{r} h_i = 0}$$

$$\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, \bigwedge_{i=1}^{r} h_i = 0\,(\mathrm{DC})$$

5.2 Performance and Limitations

Unlike with purely automated methods, such as $\mathrm{DRI}_{\wedge}$, knowledge about the system is often crucial for differential cuts to be effective; however, this knowledge can sometimes be used to construct proofs that are more computationally efficient. We have identified an example (shown in Ex. 3) with 13 state variables which defeats the current implementation of $\mathrm{DRI}_{\wedge}$ and which is easily provable using differential cuts together with both $\mathrm{DI}_{=}$ and Lie (solved quickly by running $\mathrm{DCSearch}$). Though very much an artificial problem, it demonstrates that structure in the problem can sometimes be exploited to yield efficient proofs using DC. This is especially useful for large systems with many variables where the structure of the problem is well-understood. Additionally, we see that a combination of proof rules ($\mathrm{DI}_{=}, \mathrm{Lie}, \mathrm{DC}$) can be both helpful and efficient.

Example 3. *Consider the system*

$$
\begin{aligned}
\dot{x}_1 &= -292x_7(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_2 &= -292x_8(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_3 &= -42(2x_{10}+2x_{10}^3+2x_9)(-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{41},\\
\dot{x}_4 &= -42(12x_{10}+4x_{10}^3+2x_9+6x_{10}^2x_9)(-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{41},\\
\dot{x}_5 &= -2x_{13}(-1+x_{13}+x_{11}x_{13}),\\
\dot{x}_6 &= -2x_{12}(-1+x_{12}+x_{11}x_{12}),\\
\dot{x}_7 &= 26(-6x_1x_2^2+4x_1^3x_2^2+2x_1x_2^4)(1-3x_1^2x_2^2+x_1^4x_2^2+x_1^2x_2^4)^{25},\\
\dot{x}_8 &= 26(-6x_1^2x_2+2x_1^4x_2+4x_1^2x_2^3)(1-3x_1^2x_2^2+x_1^4x_2^2+x_1^2x_2^4)^{25},\\
\dot{x}_9 &= 14(4x_3^3x_4^2+2x_3x_4^4-6x_3x_4^2x_5^2)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{10} &= 14(2x_3^4x_4+4x_3^2x_4^3-6x_3^2x_4x_5^2)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{11} &= 14(-6x_3^2x_4^2x_5+6x_5^5)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{12} &= 292x_6(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_{13} &= -x_{13}.
\end{aligned}
$$

Suppose the invariant candidate is given by the following conjunction:

$$
\begin{aligned}
x_{13}=0 \quad \wedge \quad & ((x_1^4x_2^2+x_1^2x_2^4-3x_1^2x_2^2+1)^{13})^2 \quad +\\
& ((x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^7)^2 \quad +\\
& ((-1+x_6^2+x_7^2+x_8^2)^{73})^2 \quad +\\
& ((-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{21})^2 \quad +\\
& (x_{12}+x_{11}x_{12}-1)^2=0.
\end{aligned}
$$

By using a differential cut to restrict the evolution domain to the invariant smooth manifold $x_{13}=0$ (using the rule Lie*), one obtains a system for which the sum-of-squares conjunct is a Hamiltonian and thus a first integral; this can be easily proved to be a system invariant using the rule* $\mathrm{DI}_{=}$*. Naïvely attempting to use* $\mathrm{DRI}_{\wedge}$ *takes an unreasonable amount of time due to the high degrees involved, while the proof involving DC takes under a second for both branches, provided the right rules are selected to prove invariance of atoms.*

While differential cuts can serve to increase the deductive power of sufficient proof rules, there are invariant conjunctions of equalities for which applying DC on the conjuncts given in the problem will altogether fail to be fruitful. This is due to DCSearch relying on the fact that at least some of the conjuncts considered individually are invariants for the system, which may not be the case even if the conjunction is invariant.

6 Experiments

In this section, we empirically compare the performance of three families of proof rules for checking the invariance of conjunctions: (1) DRI-related proof rules including SoSDRI (DRI plus

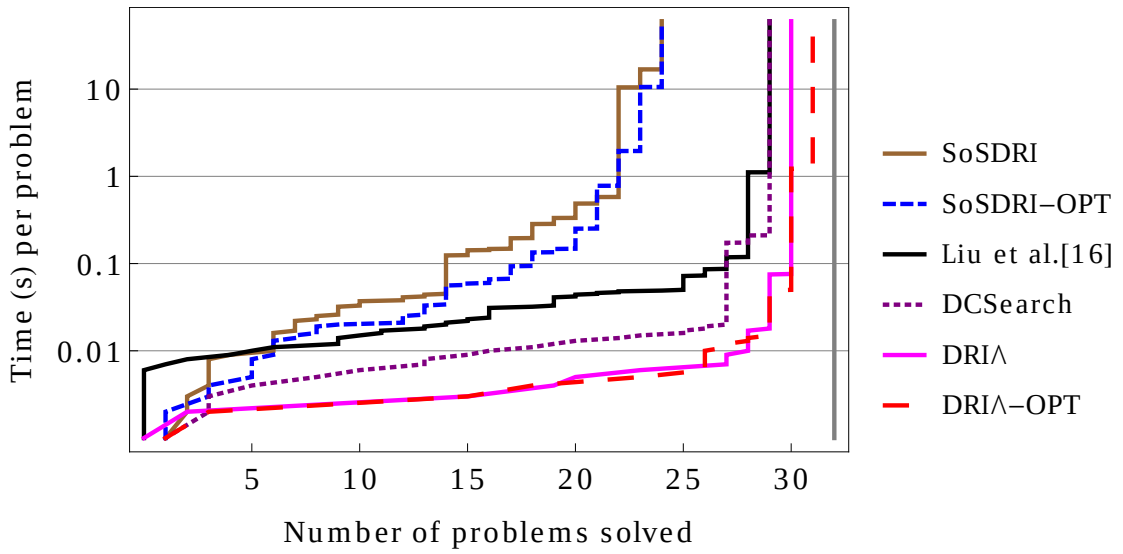

Figure 3: Empirical performance comparison of different proof rules and strategies. The total number of problems solved each in at most ts (log scale) is given in the x-axis for each method.

sum-of-squares rewriting), $\mathrm{DRI}_\wedge$ as well as their optimized versions as detailed in Section 3.3, (2) DCSearch: the differential cut proof search presented in Section 5.1, and (3) the Liu et al. procedure [21] applied to a conjunction of equalities.

We do not consider domain constraints, i.e. $H = \mathbb{R}^n$. In Fig. 3, the pair (k, t) in the plot of a proof rule P reads: the proof rule P solved k problems each in less than t seconds. The set of benchmarks contains 32 entries composed of equilibria (16), singularities (8), higher integrals (4) and abstract examples (4). The examples we used in our benchmarks originate from a number of sources - many of them come from textbooks on Dynamical Systems; others have been hand-crafted to exploit sweetspots of certain proof rules. For instance, we constructed Hamiltonian systems, systems with equilibria and systems with smooth invariants of various polynomial degrees. The most involved example has 13 state variables, a vector field with a maximum total degree of 291 and an invariant candidate with total degree of 146. It should be noted that these benchmarks are not necessarily representative, but nevertheless, an important first step towards a more comprehensive empirical analysis we hope to pursue.

For a third example, all DRI-related proof rules timed out after 60s in one example which was discharged by DCSearch in less than 6s. The detailed results are given Fig. 4. The benchmarks themselves can be found in Appendix B.

One can clearly see that for the considered set of examples, the proof rule $\mathrm{DRI}_\wedge$ is much more efficient on average compared to SoSDRI as it solves 31—out of 32—in less than 0.1s each. The optimization discussed in Section 3.3 yields a slight improvement in the performance of both SoSDRI and $\mathrm{DRI}_\wedge$. Notice that the performance imporvement is manifested more clearly when compared with SoSDRI, where the polynomials involved have large degrees. In most examples, both $\mathrm{DRI}_\wedge$ and $\mathrm{DRI}_\wedge$-OPT are very efficient. We also noticed for another example—featuring the Motzkin polynomial—that SoSDRI-OPT timed out whereas SoSDRI was able to check the

Problem	Dim	d.Inv	d.VF	SoSDRI	SoSDRI-OPT	Liu-Zhan-Zhao	DCSearch	DRI $\wedge$	DRI $\wedge$-OPT
1	1	1	1	0.000 True (N=1)	0.000 True (N=1)	0.093 True	0.000 True	0.000 True (N=1)	0.000 True (N=1)
2	1	1	3	0.000 True (N=1)	0.000 True (N=1)	0.004 True	0.001 True	0.000 True (N=1)	0.000 True (N=1)
3	1	1	3	0.006 True (N=2)	0.004 True (N=2)	0.011 True	0.003 True	0.002 True (N=1)	0.002 True (N=1)
4	2	1	2	0.002 True (N=1)	0.003 True (N=1)	0.008 True	0.005 True	0.002 True (N=1)	0.002 True (N=1)
5	2	1	4	0.035 True (N=3)	0.023 True (N=3)	0.010 True	0.004 True	0.002 True (N=1)	0.002 True (N=1)
6	3	1	3	0.030 True (N=3)	0.023 True (N=3)	0.009 True	0.004 True	0.002 True (N=1)	0.002 True (N=1)
7	2	1	5	0.042 True (N=3)	0.021 True (N=3)	0.019 True	0.014 True	0.003 True (N=1)	0.003 True (N=1)
8	3	1	2	0.149 True (N=4)	0.072 True (N=4)	0.018 True	0.006 True	0.003 True (N=1)	0.003 True (N=1)
9	3	1	2	0.020 True (N=2)	0.015 True (N=2)	0.018 True	0.007 True	0.003 True (N=1)	0.003 True (N=1)
10	3	1	2	0.026 True (N=3)	0.018 True (N=3)	0.009 True	0.005 True	0.002 True (N=1)	0.002 True (N=1)
11	4	1	4	$> 60s$ Timeout	$> 60s$ Timeout	0.036 True	0.009 True	0.005 True (N=1)	0.004 True (N=1)
12	4	1	2	0.028 True (N=2)	0.024 True (N=2)	0.034 True	0.010 True	0.005 True (N=1)	0.005 True (N=1)
13	4	1	2	$> 60s$ Timeout	1.842 True (N=5)	0.019 True	0.008 True	0.003 True (N=1)	0.003 True (N=1)
14	5	1	6	$> 60s$ Timeout	$> 60s$ Timeout	0.073 True	0.014 True	0.006 True (N=1)	0.006 True (N=1)
15	5	1	3	0.560 True (N=4)	0.692 True (N=4)	0.066 True	0.014 True	0.006 True (N=1)	0.006 True (N=1)
16	5	1	2	0.287 True (N=4)	0.069 True (N=4)	0.034 True	0.011 True	0.005 True (N=1)	0.005 True (N=1)
17	3	2	3	0.158 True (N=3)	0.055 True (N=3)	0.038 True	0.019 True	0.003 True (N=1)	0.003 True (N=1)
18	3	2	3	0.041 True (N=3)	0.022 True (N=3)	0.014 True	0.009 True	0.003 True (N=1)	0.003 True (N=1)
19	3	2	1	0.158 True (N=5)	0.100 True (N=5)	0.015 True	0.007 True	0.003 True (N=1)	0.003 True (N=1)
20	3	2	3	0.041 True (N=2)	0.041 True (N=2)	0.012 True	0.006 True	0.003 True (N=1)	0.003 True (N=1)
21	3	3	2	0.012 True (N=2)	0.011 True (N=2)	0.007 True	0.004 True	0.003 True (N=1)	0.002 True (N=1)
22	9	9	8	0.349 True (N=2)	0.303 True (N=2)	0.050 True	0.015 True	0.011 True (N=1)	0.011 True (N=1)
23	5	2	4	$> 60s$ Timeout	$> 60s$ Timeout	0.052 True	0.150 True	0.008 True (N=1)	0.008 True (N=1)
24	9	5	4	11.65 True (N=2)	11.61 True (N=2)	0.020 True	0.245 True	0.006 True (N=1)	0.006 True (N=1)
25	3	2	3	0.508 True (N=5)	0.142 True (N=5)	0.035 True	0.010 True	0.004 True (N=1)	0.004 True (N=1)
26	6	2	2	0.002 True (N=1)	0.003 True (N=1)	0.013 True	0.001 True	0.003 True (N=1)	0.003 True (N=1)
27	6	3	2	$> 60s$ Timeout	$> 60s$ Timeout	$> 60s$ Timeout	0.106 True	0.009 True (N=1)	0.008 True (N=1)
28	6	6	2	$> 60s$ Timeout	$> 60s$ Timeout	$> 60s$ Timeout	0.560 False	$> 60s$ Timeout	$> 60s$ Timeout
29	3	2	1	0.140 True (N=5)	0.127 True (N=5)	0.126 True	0.008 True	0.004 True (N=1)	0.003 True (N=1)
30	6	2	3	$> 60s$ Timeout	$> 60s$ Timeout	0.048 True	0.019 True	0.006 True (N=1)	0.006 True (N=1)
31	3	6	2	17.75 True (N=6)	$> 60s$ Timeout	0.095 True	0.058 False	0.077 True (N=3)	0.056 True (N=3)
32	13	292	291	$> 60s$ Timeout	$> 60s$ Timeout	$> 60s$ Timeout	0.003 True	$> 60s$ Timeout	$> 60s$ Timeout

Figure 4: Benchmarks

invariance in 15s.

Remark 4. *There is a slight discrepancy between the benchmarks reported in [15], which is due to a software bug that resulted in quickly falsifying example* 28 *with the optimized version of* $\mathrm{DRI}_{\wedge}$*, while all the other necessary and sufficient methods timed out.*

Example 4. *The* Motzkin polynomial*, given by*

$$M(x, y) = x^4y^2 + x^2y^4 - 3x^2y^2 + 1,$$

is often associated with Hilbert's 17^{th} *problem (see e.g. [34]). In particular, it was the first explicit example of a non-negative polynomial which is* not *a sum-of-squares. The roots of* $M(x, y)$ *are* $(1, 1), (1, -1), (-1, 1), (-1, -1) \in \mathbb{R}^2$ *. Let us consider the vector field*

$$\boldsymbol{p}(x_1, x_2) = ((x_1 - 1)(x_1 + 1), (x_2 - 1)(x_2 + 1))$$

under which the set of roots is invariant (illustrated in Fig. 5, left). Additionally, let us introduce

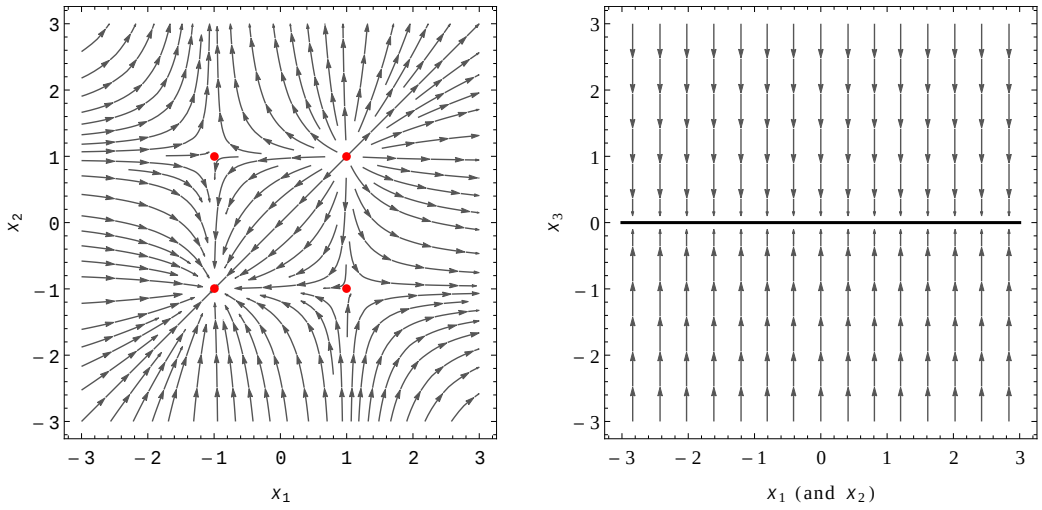

Figure 5: Invariant zero level set $M(\boldsymbol{x}) = 0$ (**left**) on an invariant sub-space in $\mathbb{R}^3$ (**right**).

an extra dimension for which we construct an invariant sub-space $x_3 = 0$ *by adding the dynamics* $\dot{x}_3 = -x_3$ *(Fig. 5, right) to yield an augmented vector field defined on* $\mathbb{R}^3$*, i.e.*

$$\boldsymbol{p}(x_1, x_2, x_3) = ((x_1 - 1)(x_1 + 1), (x_2 - 1)(x_2 + 1), -x_3)\,.$$

We can see that in this augmented system the set of states satisfying

$$M(x_1, x_2) = 0 \wedge x_3 = 0$$

is invariant under the flow of $\dot{\boldsymbol{x}} = \boldsymbol{p}(x_1, x_2, x_3)$*.*

When we investigated this example, it turned out that the rational coefficients of the remainder became more involved than those of the original polynomial before performing the reduction. For this particular example, the optimized version was able to prove invariance in $300s$ *which is* 20 *times slower than the unoptimized version.*

7 Related Work

In this paper we focus on *checking* invariance of algebraic sets under the flow of polynomial vector fields. For similar techniques used to automatically *generate* invariant algebraic sets we refer the reader to the discussion in [14].

Nagumo's Theorem [3], proved by Mitio Nagumo in 1942, characterizes invariant closed sets—a superset of algebraic sets—of locally Lipschitz-continuous vector fields—a superset of polynomial vector fields. The geometric criterion of the theorem is however intractable. The analyticity of solutions of analytic vector fields—a superset of polynomial vector fields—also gives a powerful, yet intractable, criterion to reason about invariant sets. In [35], the authors attempted to define several special cases exploiting either Nagumo's theorem or the analyticity of solutions, to give proof rules for checking invariance of (closed) semi-algebraic sets under the flow of polynomial vector fields. Liu et al. in [21] also used analyticity of solutions to polynomial ordinary differential equations and extended [35] using the ascending chain condition in Noetherian rings to ensure termination of their procedure; they gave a necessary and sufficient condition for invariance of arbitrary semi-algebraic sets under the flow of polynomial vector fields and proved the resulting conditions to be decidable.

We develop a purely algebraic approach where the ascending chain condition is also used but without resorting to local Taylor series expansions. As in [21], we require finitely many higher-order Lie derivatives to vanish; what is different, however, is the definition of the finite number each characterization requires: in [21], one is required to compute orders N_i of *each* atom h_i and to prove that all higher-order Lie derivatives of h_i, up to order $N_i - 1$, vanish. We state a weaker condition as we only require that all higher-order Lie derivatives of h_i up to order $(N - 1)$, for all i, vanish. A straightforward benefit of our characterization is the immediate reduction of the computational complexity as discussed in Section 3 and shown empirically in Section 6.

Zerz and Walcher [38] have previously considered the problem of deciding invariance of algebraic sets in polynomial vector fields; they gave a sufficient condition for checking invariance of algebraic sets which can be seen as one iteration of Algorithm 1. Therefore, Section 3 generalizes their work by providing a complete characterization of invariant algebraic sets in polynomial vector fields.

8 Conclusion

We have introduced an efficient decision procedure ($\mathrm{DRI}_\wedge$) for deciding invariance of conjunctive equational assertions for polynomial dynamical systems. We have explored the use of the differential cut rule both as a means of increasing the deductive power of existing sufficient proof rules and also as a way of constructing more computationally efficient proofs of invariance.

The empirical performance we observe in the optimized implementations of DRI and $\mathrm{DRI}_\wedge$ is very encouraging and we are confident that a proof strategy in a deductive formal verification system should give precedence to these methods. However, certain problems fall out of scope of these rules. For instance, when the problems involve transcendental functions, or still take unreasonably long time to prove. We leave these interesting questions for future work.

References

[1] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, 1996.

[2] David Bayer and Michael E. Stillman. A criterion for detecting m-regularity. *Inventiones Mathematicae*, 87:1, 1987.

[3] Franco Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[4] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real Algebraic Geometry*. A series of modern surveys in mathematics. Springer, 2010.

[5] B. Buchberger. *Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory.* Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985.

[6] George E. Collins and H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *J. Symb. Comput.*, 12(3):299–328, 1991.

[7] Patrick Cousot and Radhia Cousot. Abstract interpretation frameworks. *J. Log. Comput.*, 2(4):511–547, 1992.

[8] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms - an introduction to computational algebraic geometry and commutative algebra (2. ed.)*. Springer, 1997.

[9] Jean-Gaston Darboux. Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré. *Bulletin des Sciences Mathématiques et Astronomiques*, 2(1):151–200, 1878.

[10] Thomas Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.*, 19(4):750–773, 1990.

[11] Jean Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4) . *Journal of Pure and Applied Algebra*, 139(13):61 – 88, 1999.

[12] Jean Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[13] Khalil Ghorbal and André Platzer. Characterizing algebraic invariants by differential radical invariants. Technical Report CMU-CS-13-129, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 11 2013.

[14] Khalil Ghorbal and André Platzer. Characterizing algebraic invariants by differential radical invariants. In Erika Ábrahám and Klaus Havelund, editors, *TACAS*, volume 8413 of *Lecture Notes in Computer Science*, pages 279–294. Springer, 2014.

[15] Khalil Ghorbal, Andrew Sogokon, and André Platzer. Invariance of conjunctions of polynomial equalities for algebraic differential equations. In *SAS*, volume 8723, pages 151–168, 2014.

[16] Alain Goriely. *Integrability and Nonintegrability of Dynamical Systems*. Advanced series in nonlinear dynamics. World Scientific, 2001.

[17] David Hilbert. Über die Theorie der algebraischen Formen. *Mathematische Annalen*, 36(4):473–534, 1890.

[18] Daniel Lazard. Gröbner-bases, Gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *EUROCAL*, volume 162 of *LNCS*, pages 146–156. Springer, 1983.

[19] Sophus Lie. *Vorlesungen über continuierliche Gruppen mit Geometrischen und anderen Anwendungen*. Teubner, Leipzig, 1893.

[20] Ernest Lindelöf. Sur l'application de la méthode des approximations successives aux équations différentielles ordinaires du premier ordre. *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, 116:454–458, 1894.

[21] Jiang Liu, Naijun Zhan, and Hengjun Zhao. Computing semi-algebraic invariants for polynomial dynamical systems. In Samarjit Chakraborty, Ahmed Jerraya, Sanjoy K. Baruah, and Sebastian Fischmeister, editors, *EMSOFT*, pages 97–106. ACM, 2011.

[22] Nadir Matringe, Arnaldo Vieira Moura, and Rachid Rebiha. Generating invariants for nonlinear hybrid systems by linear algebraic methods. In Radhia Cousot and Matthieu Martel, editors, *SAS*, volume 6337 of *LNCS*, pages 373–389. Springer, 2010.

[23] Ernst W. Mayr. Membership in polynomial ideals over Q is exponential space complete. In Burkhard Monien and Robert Cori, editors, *STACS*, volume 349 of *LNCS*, pages 400–406. Springer, 1989.

[24] Ernst W Mayr and Albert R Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305 – 329, 1982.

[25] Peter J. Olver. *Applications of Lie Groups to Differential Equations*. Springer, 2000.

[26] André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reasoning*, 41(2):143–189, 2008.

[27] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010.

[28] André Platzer. *Logical Analysis of Hybrid Systems - Proving Theorems for Complex Dynamics*. Springer, 2010.

[29] André Platzer. A differential operator approach to equational differential invariants - (invited paper). In Lennart Beringer and Amy P. Felty, editors, *ITP*, volume 7406 of *LNCS*, pages 28–48. Springer, 2012.

[30] André Platzer. The structure of differential invariants and differential cut elimination. *Logical Methods in Computer Science*, 8(4):1–38, 2012.

[31] Sriram Sankaranarayanan. Automatic invariant generation for hybrid systems using ideal fixed points. In Karl Henrik Johansson and Wang Yi, editors, *HSCC*, pages 221–230. ACM, 2010.

[32] Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. Constructing invariants for hybrid systems. *Formal Methods in System Design*, 32(1):25–55, 2008.

[33] Konrad Schmüdgen. Around Hilbert's 17th problem. In M. Grötschel, editor, *Documenta Mathematica*, Optimization stories, extra volume ISMP, pages 433–438, 2012.

[34] Ankur Taly and Ashish Tiwari. Deductive verification of continuous dynamical systems. In Ravi Kannan and K. Narayan Kumar, editors, *FSTTCS*, volume 4 of *LIPIcs*, pages 383–394. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2009.

[35] Alfred Tarski. A decision method for elementary algebra and geometry. *Bulletin of the American Mathematical Society*, 59, 1951.

[36] Wolfgang Walter. *Ordinary Differential Equations*. Graduate Texts in Mathematics. Springer New York, 1998.

[37] Eva Zerz and Sebastian Walcher. Controlled invariant hypersurfaces of polynomial control systems. *Qualitative Theory of Dynamical Systems*, 11(1):145–158, 2012.

A Proof of Theorem 3

In [13, Theorem 2], we characterized the invariance of a polynomial equality—of the form $h = 0$—for a polynomial vector field $\dot{\boldsymbol{x}} = p(\boldsymbol{x})$. The purpose of this section is to prove Theorem 3 (Section 3), an extension of [13, Theorem 2] to a conjunction of polynomial equalities, i.e. $h_1 = 0 \wedge h_2 = 0 \wedge \cdots \wedge h_r = 0$. We first recall some basic definitions and known results (Section A.1). The proof is then given in Section A.2. Unless otherwise specified, the evolution domain H will be considered as an open set of $\mathbb{R}^n$.

A.1 Preliminaries

Polynomial functions are smooth (C^∞, i.e. they have derivatives of any order), they are locally Lipschitz-continuous. By Cauchy-Lipschitz theorem (a.k.a. Picard-Lindelöf theorem) [20], the initial value problem $(\dot{\boldsymbol{x}} = \boldsymbol{p}, \boldsymbol{x}(0) = \boldsymbol{x}_\iota)$, for some $\boldsymbol{x}_\iota \in \mathbb{R}^n$, admits a unique maximal solution $\boldsymbol{x}(t)$ defined for $t \in U$, where U is some nonempty open set (interval) in $\mathbb{R}$ that contains zero.

The orbit of $\boldsymbol{x}(t)$ is defined as follows:

Definition 2 (Orbit)**.** *The* orbit *of the solution of Def. 1, $\boldsymbol{x}(t)$ is defined as*

$$\mathcal{O}(\boldsymbol{x}_\iota) \stackrel{\text{def}}{=} \{\boldsymbol{x}(t) \mid t \in U\} \subseteq \mathbb{R}^n \ .$$

Since we are interested in forward reachability, we restrict in addition the orbit to non-negative time:

Definition 3 (Positive Orbit)**.** *The* positive orbit*, or reachable set, of the solution of Def. 1, $\boldsymbol{x}(t)$ is defined as*

$$\mathcal{O}^+(\boldsymbol{x}_\iota) \stackrel{\text{def}}{=} \{\boldsymbol{x}(t) \mid t \in U \cap [0, +\infty]\} \subseteq \mathbb{R}^n \ .$$

In the presence of an open evolution domain $H \subseteq \mathbb{R}^n$, we require that $\boldsymbol{x}_\iota \in H$ and we restrict the orbit $\mathcal{O}^+(\boldsymbol{x}_\iota)$ to H, that is, we are only interested in the portion of the trajectory that remains inside H.

$$\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H} \stackrel{\text{def}}{=} \{\boldsymbol{x}(t) \mid t \in U \cap [0, +\infty] \wedge \forall t' \in [0, t] : x(t') \in H\} \ .$$

Definition 4 (Ideal)**.** *An* ideal *I is a subset of $\mathbb{R}[\boldsymbol{x}]$ that contains the polynomial zero (0), is stable under addition, and external multiplication. That is, for all $h_1, h_2 \in I$, the sum $h_1 + h_2 \in I$; and if $h \in I$, then, $qh \in I$, for all $q \in \mathbb{R}[\boldsymbol{x}]$.*

For a finite natural number r, we denote by $\langle h_1, \ldots, h_r \rangle$ the subset of $\mathbb{R}[\boldsymbol{x}]$ generated by the polynomials $\{h_1, \ldots, h_r\}$, i.e. the set of linear combinations of the polynomials h_i (where the coefficients are themselves polynomials):

$$\langle h_1, \ldots, h_r \rangle \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{r} q_i h_i \mid q_1, \ldots, q_r \in \mathbb{R}[\boldsymbol{x}] \right\} \ .$$

By Def. 4, the set $\langle h_1, \ldots, h_r \rangle$ is an ideal. More interestingly, by Hilbert's Basis Theorem [17], any ideal I of the Noetherian ring $\mathbb{R}[\boldsymbol{x}]$ can be *generated* by a finite set of polynomials, $\{h_1, \ldots, h_r\}$, so that $I = \langle h_1, \ldots, h_r \rangle$.

Definition 5 (Variety or Algebraic Set or Zeros Set)**.** *Given $Y \subseteq \mathbb{R}[\boldsymbol{x}]$, the* variety *(over the reals), $V(Y)$, is a subset of $\mathbb{R}^n$ defined by the common roots of all polynomials in Y. That is,*

$$V(Y) \stackrel{\text{def}}{=} \left\{ \boldsymbol{x} \in \mathbb{R}^n \mid \forall h \in Y, h(\boldsymbol{x}) = 0 \right\} \ .$$

$V(\cdot)$ can be thought of as an operator that maps subsets of $\mathbb{R}[\boldsymbol{x}]$ to subsets of $\mathbb{R}^n$. In general, the map $V(\cdot)$ is not injective even when applied to ideals: two distinct subsets of $\mathbb{R}[\boldsymbol{x}]$ can be mapped to the exact same variety. For instance, in $\mathbb{R}[x_1, x_2]$, the ideals $I_1 = \langle x_1, x_2^2 \rangle$ and $I_2 = \langle x_1^2, x_2 \rangle$, are mapped to the point $(x_1, x_2) = (0, 0)$ (which is a variety). The ideals I_1 and I_2 are distinct and incomparable: the polynomial $x_1 \in I_1$ is not in I_2 but $x_2 \in I_2$ is not in I_1.

Definition 6 (Vanishing Ideal)**.** *The* vanishing ideal *(over the reals), $I(S)$, of $S \subseteq \mathbb{R}^n$ is the set of all polynomials that evaluates to zero for all $\boldsymbol{x} \in S$:*

$$I(S) \stackrel{\text{def}}{=} \left\{ h \in \mathbb{R}[\boldsymbol{x}] \mid \forall \boldsymbol{x} \in S, h(\boldsymbol{x}) = 0 \right\} \ . \tag{13}$$

The set $I(S) \subseteq \mathbb{R}[\boldsymbol{x}]$ is an ideal as it satisfies the requirements of Def. 4. Likewise, we can think of $I(\cdot)$ (Def. 6) as a non-injective operator that acts on subsets of $\mathbb{R}^n$. For instance, the two intervals $[1, 2]$ and $[-2, -1]$ are subsets of $\mathbb{R}$ mapped to the same ideal, namely $\langle 0 \rangle$. However, when restricted to varieties, the operator $I(\cdot)$ is injective.

We state the following well-known result (see, e.g. [8, Chapter 4, Theorem 7]) for convenience as it permits to switch back and forth between varieties of $\mathbb{R}^n$ and ideals of $\mathbb{R}[\boldsymbol{x}]$.

Proposition 3 (Ideal-Variety Correspondence)**.** *For any ideals I_1 and I_2 of $\mathbb{R}[\boldsymbol{x}]$, if $I_1 \subseteq I_2$, then $V(I_1) \supseteq V(I_2)$. Likewise, for any varieties V_1 and V_2 of $\mathbb{R}^n$, if $V_1 \subseteq V_2$, then $I(V_1) \supseteq I(V_2)$. Furthermore, for any variety S, we have $V(I(S)) = S$ and for any ideal Y, we have $Y \subseteq I(V(Y))$.*

The Zariski closure $\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$ of the set $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$ is the variety of the vanishing ideal of $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$:

$$\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H} \stackrel{\text{def}}{=} V(I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})) \ . \tag{14}$$

That is, $\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$ is defined as the set of all points that are common roots of all polynomials that are zero everywhere in $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$.

Proposition 4 (Soundness of Zariski Closure)**.** $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H} \subseteq \bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$.

Proof. All points of $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$ are roots of some polynomial in its vanishing ideal $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ (Def. 6), and all roots of all polynomials in $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ are in $\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$ (Def. 5). Thus, $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H} \subseteq V(I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})) = \bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$[4]. □

[4]NB: If we use an algebraically closed field instead of $\mathbb{R}$, the operators $V(.)$ and $I(.)$ form a Galois connection. One can therefore talk about exact abstraction, where subsets of the space are abstracted by varieties. Since we use the real numbers field, which is not closed, we technically only have a concretisation-based abstraction [7].

Lie derivatives (Eq. (3)) are closely related to time derivatives. In fact, they are equal when evaluated on the solution $\boldsymbol{x}(t)$.

Lemma 3 (Derivation)**.** *Let $h \in \mathbb{R}[\boldsymbol{x}]$. Then, the Lie derivative of h along the vector field $\boldsymbol{p}$ is exactly equal to the time derivative of $h(\boldsymbol{x}(t))$.*

$$\mathfrak{L}_{\boldsymbol{p}}(h) = \frac{dh(\boldsymbol{x}(t))}{dt} = \dot{h} \ .$$

Proof. The lemma follows from the chain rule: the polynomial h is seen as a function of $\boldsymbol{x}$ which is in turn a function of t (when $\boldsymbol{x}(t)$ is the solution of the initial value problem $(\dot{\boldsymbol{x}} = \boldsymbol{p}, \boldsymbol{x}(0) = \boldsymbol{x}_\iota)$. Thus,

$$\dot{h} = \frac{d}{dt}h(\boldsymbol{x}(t)) = \sum \frac{\partial h}{\partial x_i}\dot{x_i}(t) = \mathfrak{L}_{\boldsymbol{p}}(h) \ .$$

□

The time derivation gives an analytic point of view, whereas the Lie derivative is purely algebraic and makes explicit the link to the vector field. Lie derivation allows, therefore, to compute symbolically the time derivative of any polynomial $h \in \mathbb{R}[\boldsymbol{x}]$: it only requires the partial derivatives of h and the vector field $\boldsymbol{p}$.

Definition 7 (Real Ideal [4, Definition 4.1.3])**.** *An ideal I of $\mathbb{R}[\boldsymbol{x}]$ is said to be* real *if and only if for every sequence $q_1, \ldots, q_r$ of elements of $\mathbb{R}[\boldsymbol{x}]$, we have*

$$q_1^2 + \cdots + q_r^2 \in I \longrightarrow q_i \in I, \text{ for } i = 1, \ldots, r \ .$$

In particular, all vanishing ideals are real ideals.

Lemma 4. *The vanishing ideal $I(S)$ of any $S \subseteq \mathbb{R}^n$ is a real ideal.*

Proof. If the polynomial $q_1^2 + \cdots + q_r^2$ is in $I(S)$, for some $q_1, \ldots, q_r \in \mathbb{R}[\boldsymbol{x}]$, then its set of roots contain S (Def. 6). However, we have the following equivalence over the reals

$$q_1^2 + \cdots + q_r^2 = 0 \leftrightarrow q_i = 0, \text{ for } i = 1, \ldots, r \ .$$

Thus, a root of the polynomial $q_1^2 + \cdots + q_r^2$ is also a root of the polynomials q_i, for $i = 1, \ldots, r$. This means that $q_i \in I(S)$ for $i = 1, \ldots, r$. By Def. 7, $I(S)$ is a real ideal. □

In $\mathbb{R}[\boldsymbol{x}]$, real ideals have an important property, they are fixed under the mapping $I(V(\cdot))$ (see Def. 6 and Def. 5).

Proposition 5 (Real Nullstellensatz [4, Theorem 4.1.4])**.** *Let Y be an ideal of $\mathbb{R}[\boldsymbol{x}]$. Then, $Y = I(V(Y))$ if and only if Y is real.*

Definition 8 (Invariant Regions subject to evolution domain constraints)**.** *The region $S \subseteq \mathbb{R}^n$ is (positively) invariant for the vector field $\boldsymbol{p}$ subject to the evolution domain constraint H if and only if*

$$\forall \boldsymbol{x}_\iota \in S \cap H, \mathcal{O}^+(\boldsymbol{x}_\iota)_{|H} \subseteq S \ .$$

In particular, we focus on invariant algebraic sets, that is, where S is a variety. This choice is essentially motivated by the interesting algebraic properties of varieties. As a matter of fact, when S is a variety, the (intractable) orbit $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$ in Def. 8 can be equivalently substituted by its closure $\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$ allowing a powerful algebraic handle for invariant varieties.

Lemma 5. *The variety S is a positive invariant variety for the vector field $\boldsymbol{p}$ subject to the evolution domain constraint H, if and only if*

$$\forall \boldsymbol{x}_\iota \in S \cap H, \bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H} \subseteq S \ .$$

Proof. If S is an invariant variety subject to H then, for all $\boldsymbol{x}_\iota \in S \cap H$, $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H} \subseteq S$ (Def. 8). However, $\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$ is the smallest variety containing $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$. Therefore, $\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H} \subseteq S$.

On the other hand, since $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H} \subseteq \bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$ (Prop. 4), then $\bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H} \subseteq S$ implies $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H} \subseteq S$. □

We state an important property of the vanishing ideal $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$. Similar results are known under different formulations ([32, Theorem 3.1], [29, Lemma 3.7] and [13, Proposition 3]).

Proposition 6. *$I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ is a differential ideal for $\mathfrak{L}_{\boldsymbol{p}}$, i.e. it is stable under the action of the $\mathfrak{L}_{\boldsymbol{p}}$ operator: for all $h \in I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$, $\mathfrak{L}_{\boldsymbol{p}}(h) \in I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$.*

Proof. Let I denote $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$. Given $h \in I$, we prove that $\mathfrak{L}_{\boldsymbol{p}}(h) \in I$. If h is in I, then the vector $\boldsymbol{x}(t)$ is a root of the polynomial $h(\boldsymbol{x})$. This means that the real-valued function $h(\boldsymbol{x}(t))$—obtained by substituting $\boldsymbol{x}$ in h by the solution $\boldsymbol{x}(t)$—is a constant function and is actually equal to zero over an open interval containing 0. The existence of such an open interval follows immediately from three facts: $\boldsymbol{x}_\iota \in H$, $x(t)$ is defined over an open interval U containing 0, and that H is an open set. Its time derivative is therefore also zero for all $\boldsymbol{x}(t) \in \mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$. Since the time derivative of $h(\boldsymbol{x}(t))$ corresponds exactly to the Lie derivative of h, it follows that for all $\boldsymbol{x}(t) \in \mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$, $\boldsymbol{x}(t)$ is a zero of $\mathfrak{L}_{\boldsymbol{p}}(h)$—seen as a polynomial of $\mathbb{R}[\boldsymbol{x}]$. Therefore, $\mathfrak{L}_{\boldsymbol{p}}(h) \in I$, by definition of I. □

Notice that the fact that H is an open set plays a crucial role in this proposition. In fact the statement does no longer hold for an arbitrary (or even closed) set H.

Example 5. *Consider the vector field $\boldsymbol{p} = (-x_2, x_1)$ and the evolution domain constraint $H := x_1 \leq -1$. When $\boldsymbol{x}_\iota = (-1, 0)$, $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$ is reduced to one point, namely $(-1, 0)$ and therefore, $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}) = \langle x_1 + 1, x_2 \rangle$. The polynomial $h = x_2$ is trivially in $\langle x_1 + 1, x_2 \rangle$, however, its Lie derivative $\mathfrak{L}_{\boldsymbol{p}}(h) = x_1$ is not. This suggests that the proposition may fail whenever $\boldsymbol{x}_\iota$ is on the boundaries of H.*

A.2 Proof of the Main Result

The *differential radical* of an ideal generated by one polynomial (principal ideal) $\langle h \rangle$ can be extended to a generic ideal $J = \langle h_1, \ldots, h_r \rangle \subseteq \mathbb{R}[\boldsymbol{x}]$. Since the ring of polynomials over $\mathbb{R}$ is

Noetherian, the following chain of ideals:

$$\begin{aligned}\langle h_1,\dots,h_r\rangle &\subset \langle h_1,\dots,h_r,\mathfrak{L}_{\boldsymbol{p}}^{(1)}(h_1),\dots,\mathfrak{L}_{\boldsymbol{p}}^{(1)}(h_r)\rangle\\ &\subset \cdots \subset \langle h_1,\dots,h_r,\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_1),\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_r)\rangle\\ &= \langle h_1,\dots,h_r,\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h_1),\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h_r)\rangle \ .\end{aligned}$$

has necessarily a finite length. The construction of such ascending chain is very similar to the construction of the radical of an ideal[5], except with higher-order Lie derivatives, $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j)$, in place of higher powers of polynomials, h_j^i. This motivates the following definition.

Definition 9 (Differential Radical Ideal)**.** *For $\langle h_1,\dots,h_r\rangle \subseteq \mathbb{R}[\boldsymbol{x}]$, let $1 \leq N < \infty$ be the smallest natural number such that:*

$$\forall j = 1,\dots,r \quad \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h_j) \in \langle h_1,\dots,h_r,\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_1),\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_r)\rangle \ . \tag{15}$$

We call the ideal

$$\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_1,\dots,h_r\rangle} \stackrel{\text{def}}{=} \langle h_1,\dots,h_r,\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_1),\dots,\mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_r)\rangle, \tag{16}$$

the differential radical ideal *of $h_1,\dots,h_r$. N will be referred to as the* differential radical order*, or simply order, of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_1,\dots,h_r\rangle}$.*

Def. 9 extends the concept of differential radical order introduced, for one polynomial, in [13, Definition 8]. Differential radical order is akin to the concept of *rank* used in [21, Theorems 14 & 15].

Theorem 3 (Conjunctive Differential Radical Characterization)**.** *Let $h_1,\dots,h_r \in \mathbb{R}[\boldsymbol{x}]$ and let H denote some* open *evolution domain constraint. Then, the conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, is invariant under the flow of the vector field $\boldsymbol{p}$, subject to the evolution constraint H, if and only if*

$$H \vdash \bigwedge_{j=1}^{r} h_j = 0 \rightarrow \bigwedge_{j=1}^{r}\bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j) = 0 \ . \tag{17}$$

where N denotes the order of the conjunction.

Proof. The proof follows the same steps of [13, Theorem 1] while generalizing it to higher-dimensions. Typically, the vector $\boldsymbol{g}$ below is formed by concatenating r vectors, and the matrix $A(t)$ is a block matrix.

Necessary condition. Let $\langle h_1,\dots,h_r\rangle \subseteq I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$. By Prop. 6, all higher-order Lie derivatives of all h_j are also in $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$. Eq. (17) follows from the fact that all polynomials of $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ vanish on all points of $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$, in particular for $\boldsymbol{x}_\iota$, since $\boldsymbol{x}_\iota \in \mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$.

Sufficient condition. We prove that if Eq. (17) is satisfied then $h_1(\boldsymbol{x}(t)) = 0,\dots,h_r(\boldsymbol{x}(t)) = 0$ for all $\boldsymbol{x}(t) \in \mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$, which implies that the ideal $\langle h_1,\dots,h_r\rangle \subseteq I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ by definition

[5]For a principal ideal, $\langle h\rangle$, the construction of its radical ideal, $\sqrt{\langle h\rangle}$ consists of augmenting $\langle h\rangle$ by all high powers h^i of the generating element h.

of $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ (Def. 6). Recall that U is the domain of definition (some open interval of $\mathbb{R}$) for t of the solution $\boldsymbol{x}(t)$. We will denote by $U_{|H}$ the restriction of U to H: $U_{|H} = \{t \mid \boldsymbol{x}(t) \in H\}$.

We define the real functions $f_j : U_{|H} \to \mathbb{R}$ by: $f_j(t) = h_j(\boldsymbol{x}(t))$. We want to prove that the functions f_j are identically zero on $U_{|H}$. Since N is the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_1, \ldots, h_r \rangle}$, by Eq. (15) (Def. 9), for each h_j, there exists a vector of polynomials $\boldsymbol{q}_{ij}(\boldsymbol{x})$ such that

$$\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h_j) - \sum_{i=0}^{N-1} \boldsymbol{q}_{ij} \cdot (\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_1), \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_r)) = 0 \ . \tag{18}$$

Let $\boldsymbol{\alpha}_{ij} : U_{|H} \to \mathbb{R}^r$; $t \mapsto \boldsymbol{q}_{ij}(\boldsymbol{x}(t))$. The equality of Eq. (18), together with the initial value condition given by Eq. (17), can be transformed into the following homogeneous higher-order higher-dimension linear differential equation.

$$\begin{aligned} \boldsymbol{f}^{(N)}(t) - \sum_{i=0}^{N-1} A_i(t) \boldsymbol{f}^{(i)}(t) = 0, \\ \boldsymbol{f}^{(0)}(0) = \boldsymbol{f}^{(1)}(0) = \cdots = \boldsymbol{f}^{(N-1)}(0) = 0, \end{aligned} \tag{19}$$

where $\boldsymbol{f} = (f_1, \ldots, f_r)$ and the $r \times r$ square matrices $A_i(t)$ are such that the jth row of $A_i(t)$ is the vector $\boldsymbol{\alpha}_{ij}$.

The newly defined system in Eq. (19) can be seen as an Nr dimensional linear nonautonomous ($A_i(t)$ are time dependent) system using the encoding $\boldsymbol{g} = \left(\boldsymbol{f}^{(0)}, \ldots, \boldsymbol{f}^{(N-1)}\right)$, that is, $\boldsymbol{g}$ is the vector obtained by concatenating the N vectors $\boldsymbol{f}^{(i)}$:

$$\dot{\boldsymbol{g}} - A(t)\boldsymbol{g} = \boldsymbol{0}, \tag{20}$$

where,

$$A(t) = \begin{pmatrix} 0 & I_r & 0 & \cdots & 0 \\ 0 & 0 & I_r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & I_r \\ A_0(t) & A_1(t) & \cdots & A_{N-2}(t) & A_{N-1}(t) \end{pmatrix} \ .$$

I_r denotes the identity matrix of dimension r. In the newly defined linear system of Eq. (20), $A(t)\boldsymbol{g}$ is globally Lipschitz continuous, w.r.t. $\boldsymbol{g}$. That is, there exists a global Lipschitz constant, namely $\|A(t)\|$, the induced norm of $\mathbb{R}^{Nr}$ on the $\mathbb{R}^{Nr \times Nr}$ space, such that, for all t:

$$\forall \boldsymbol{g}_1, \boldsymbol{g}_2 \in \mathbb{R}^{Nr}, \quad \|A(t)\boldsymbol{g}_1 - A(t)\boldsymbol{g}_2\| \leq \|A(t)\|\|\boldsymbol{g}_1 - \boldsymbol{g}_2\| \ .$$

By Cauchy-Lipschitz theorem [20] (see [37, Chapter 14, Theorem VI] for the multi-linear case), there exists a unique solution $\boldsymbol{g}(t)$ defined on the entire interval $U_{|H}$ ($A_i(t)$, and hence $A(t)$, are not defined outside $U_{|H}$ by definition), that satisfies the initial condition $\boldsymbol{g}(0) = \boldsymbol{0}$. However, the null function, $\boldsymbol{g}(t) = \boldsymbol{0}$ is an obvious solution to Eq. (20), which satisfies $\boldsymbol{g}(0) = \boldsymbol{0}$. Hence, $\boldsymbol{g}(t)$ is identically zero for all $t \in U_{|H}$. Since $\boldsymbol{g} = \left(\boldsymbol{f}^{(0)}, \ldots, \boldsymbol{f}^{(N-1)}\right)$, by Lem. 3, for all $i = 0 \ldots N-1$, for all $j = 1 \ldots r$, $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j)(\boldsymbol{x}(t)) = 0$ for all $\boldsymbol{x}(t)$. Therefore, all the polynomials h_j as well as all their Lie derivatives vanish on the set $\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}$ and are hence members of $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$. □

We finally prove Theorem 3. For convenience, we first recall the theorem.

Theorem (Conjunctive Differential Radical Characterization)**.** *Let $h_1, \ldots, h_r \in \mathbb{R}[\boldsymbol{x}]$. Then, the conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, is invariant under the flow of the vector field $\boldsymbol{p}$ subject to the evolution domain constraint H, if and only if*

$$\Big(H \wedge \bigwedge_{j=1}^{r} h_j = 0\Big) \rightarrow \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j) = 0 \ . \tag{21}$$

where N denotes the order of the ideal $\langle h_1, \ldots, h_r \rangle$.

Proof. Necessary Condition. Let $\boldsymbol{x}_\iota \in H$ be a root of all h_j, $j = 1 \ldots r$ (i.e. $\boldsymbol{x}_\iota \in V(\langle h_1, \ldots, h_r \rangle)$). If $V(\langle h_1, \ldots, h_r \rangle)$ is an invariant variety subject to H, then by Lem. 5

$$V(I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})) = \bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H} \subseteq V(\langle h_1, \ldots, h_r \rangle),$$

and therefore $I(V(I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}))) \supseteq I(V(\langle h_1, \ldots, h_r \rangle))$ (Prop. 3).

We know that $I(V(\langle h_1, \ldots, h_r \rangle)) \supseteq \langle h_1, \ldots, h_r \rangle$ and that $I(V(I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}))) = I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ (from Lem. 4, $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ is a real ideal, the equality follows from the real Nullstellensatz stated in Prop. 5), hence $I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H}) \supseteq \langle h_1, \ldots, h_r \rangle$. By Theorem **??**, this implies Eq. (17), and, therefore, Eq. (21) holds.

Sufficient Condition. The initial condition $\boldsymbol{x}_\iota$ satisfies Eq. (17) of Theorem **??** by hypothesis, which implies $\langle h_1, \ldots, h_r \rangle \subseteq I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})$ by Theorem **??**. But then by Prop. 3, $V(\langle h_1, \ldots, h_r \rangle) \supseteq V(I(\mathcal{O}^+(\boldsymbol{x}_\iota)_{|H})) = \bar{\mathcal{O}}^+(\boldsymbol{x}_\iota)_{|H}$. The conclusion follows by Lem. 5: $V(\langle h_1, \ldots, h_r \rangle$ is an invariant region subject to the evolution domain H. □

Eq. (21) can be restated using sequent calculus, where $F \vdash G$ means that whenever the boolean formula F (antecedent) is satisfied, then the boolean formula G is true. Eq. (21) can therefore be rewritten as follows:

$$H \vdash \bigwedge_{j=1}^{r} h_j = 0 \rightarrow \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j) = 0 \ .$$

This reformulation—used in Theorem 3—is more suitable for the main theme of the presented paper: developing and extending proof calculus for hybrid systems.

B Benchmarks

For all examples the constraint evolution domain H is set to $\mathbb{R}^n$. For each problem, The left hand side equation gives the candidate to check. The right hand side gives the vector field $\boldsymbol{p}$.

1	
$x_1{=}0$	$\dot{x_1} = x_1$
2	
$x_1{=}0$	$\dot{x_1} = x_1^3$
3	
$x_1{-}1{=}0 \wedge x_1{+}1{=}0$	$\dot{x_1} = (x_1 - 1)(x_1 + 1)(x_1 + 3)$
4	
$x_1{-}1{=}0 \wedge x_2{+}1{=}0$	$\dot{x_1} = (x_1 - 1)x_2$ $\dot{x_2} = x_2(x_2 + 1)$
5	
$x_1{-}1{=}0 \wedge x_2{-}1{=}0$	$\dot{x_1} = (x_1 - 1)x_1x_2$ $\dot{x_2} = (x_2 - 1)x_2^3$
6	
$x_1{-}1{=}0 \wedge x_3{-}4{=}0$	$\dot{x_1} = (x_1 - 1)x_3^2$ $\dot{x_2} = x_1x_2$ $\dot{x_3} = x_1(x_3 - 4)$
7	
$x_1{=}0 \wedge x_2{=}0$	$\dot{x_1} = x_2^5 + x_1^2(x_2 - x_1)$ $\dot{x_2} = -2x_1x_2^2(2x_1^2 + x_2^2 - 3)$
8	
$x_1{-}1{=}0 \wedge x_2{+}1{=}0 \wedge x_3{-}4{=}0$	$\dot{x_1} = (x_1 - 1)^2$ $\dot{x_2} = x_1(x_2 + 1)$ $\dot{x_3} = x_2(x_3 - 4)$
9	
$x_1{-}1{=}0 \wedge x_2{-}1{=}0 \wedge x_3{-}4{=}0$	$\dot{x_1} = (x_1 - 1)x_2$ $\dot{x_2} = (x_2 - 1)x_2$ $\dot{x_3} = x_1(x_3 - 4)$
10	
$x_1{-}1{=}0 \wedge x_3{-}4{=}0$	$\dot{x_1} = (x_1 - 1)x_3$ $\dot{x_2} = x_2$ $\dot{x_3} = x_1(x_3 - 4)$
11	
$x_1{-}1{=}0 \wedge x_2{+}1{=}0 \wedge x_3{-}4{=}0 \wedge x_4{-}4{=}0$	$\dot{x_1} = (x_1 - 1)x_2$ $\dot{x_2} = x_1(x_2 + 1)$ $\dot{x_3} = x_1(x_3 - 4)$ $\dot{x_4} = (x_4 - 4)^4$
12	
$x_1{-}1{=}0 \wedge x_2{-}1{=}0 \wedge x_3{-}4{=}0 \wedge x_4{-}1{=}0$	$\dot{x_1} = (x_1 - 1)x_2$ $\dot{x_2} = (x_2 - 1)x_2$ $\dot{x_3} = x_1(x_3 - 4)$ $\dot{x_4} = x_1(x_4 - 1)$
13	
$x_1{-}1{=}0 \wedge x_3{-}4{=}0 \wedge x_4{-}4{=}0$	$\dot{x_1} = (x_1 - 1)x_2$ $\dot{x_2} = x_2$ $\dot{x_3} = (x_3 - 4)x_3$ $\dot{x_4} = x_1(x_4 - 4)$
14	

$x_1{-}1{=}0 \wedge x_2{+}1{=}0 \wedge x_3{-}4{=}0 \wedge x_4{-}4{=}0 \wedge x_5{-}2{=}0$	$\dot{x_1} = (x_1 - 1)x_2$ $\dot{x_2} = x_1(x_2 + 1)$ $\dot{x_3} = x_2(x_3 - 4)$ $\dot{x_4} = (x_4 - 4)^6$ $\dot{x_5} = (x_5 - 2)^3$
15	
$x_1{-}1{=}0 \wedge x_2{-}1{=}0 \wedge x_3{-}4{=}0 \wedge x_4{-}1{=}0 \wedge x_5{+}2{=}0$	$\dot{x_1} = (x_1 - 1)^2$ $\dot{x_2} = (x_2 - 1)^3$ $\dot{x_3} = x_2(x_3 - 4)$ $\dot{x_4} = x_2(x_4 - 1)$ $\dot{x_5} = x_2(x_5 + 2)$
16	
$x_1{-}1{=}0 \wedge x_3{-}4{=}0 \wedge x_4{-}4{=}0 \wedge x_5{-}1{=}0$	$\dot{x_1} = (x_1 - 1)x_2$ $\dot{x_2} = x_1$ $\dot{x_3} = x_2(x_3 - 4)$ $\dot{x_4} = x_2(x_4 - 4)$ $\dot{x_5} = x_1(x_5 - 1)$
17	
$x_1^2{+}x_2^2{+}x_3^2{-}1{=}0 \wedge x_3{=}0$	$\dot{x_1} = x_1(-x_1^2 - x_2^2 + 1) - x_2$ $\dot{x_2} = x_1 + x_2(-x_1^2 - x_2^2 + 1)$ $\dot{x_3} = x_3$
18	
$x_1^2{+}x_2^2{-}1{=}0 \wedge x_3{=}0$	$\dot{x_1} = x_1(-x_1^2 - x_2^2 + 1) - x_2$ $\dot{x_2} = x_1 + x_2(-x_1^2 - x_2^2 + 1)$ $\dot{x_3} = x_3$
19	
$x_1^2{+}x_2^2{-}1{=}0 \wedge x_3{-}x_1{=}0$	$\dot{x_1} = -x_2$ $\dot{x_2} = x_3$ $\dot{x_3} = -x_2$
20	
$x_1x_3{+}x_3{-}1{=}0 \wedge x_2{-}x_1^2{=}0$	$\dot{x_1} = x_2 + x_3$ $\dot{x_2} = 2x_1x_2 + 2x_1x_3$ $\dot{x_3} = -x_3^3 - x_2x_3^2$
21	
$x_1^3{+}x_1^2{-}x_2^2{=}0 \wedge x_3{=}0$	$\dot{x_1} = -2x_2$ $\dot{x_2} = -3x_1^2 - 2x_1$ $\dot{x_3} = -x_3$
22	
$27x_1^7{+}12x_4x_5^2x_1{-}(x_6x_5^2{+}x_1)^3{+}x_2(x_7{-}3)^3{-}\frac{x_8^3}{5}{-}(-16x_4^2{+}x_1{+}77x_1x_2{+}3x_1x_2x_3)^2{=}0 \wedge x_9{=}0$	$\dot{x_1} = 6x_5x_6(x_6x_5^2 + x_1)^2 - 24x_1x_4x_5$ $\dot{x_2} = 3x_5^2(x_6x_5^2 + x_1)^2$ $\dot{x_3} = -3x_2(x_7 - 3)^2$ $\dot{x_4} = \frac{3x_8^2}{5}$ $\dot{x_5} = 189x_1^6 + 12x_4x_5^2 - 3(x_6x_5^2 + x_1)^2$ $\quad - 2(3x_3x_2 + 77x_2 + 1)(-16x_4^2 + x_1 + 77x_1x_2 + 3x_1x_2x_3)$ $\dot{x_6} = (x_7 - 3)^3 - 2(3x_3x_1 + 77x_1)(-16x_4^2 + x_1 + 77x_1x_2 + 3x_1x_2x_3)$ $\dot{x_7} = -6x_1x_2(-16x_4^2 + x_1 + 77x_1x_2 + 3x_1x_2x_3)$ $\dot{x_8} = 12x_1x_5^2 + 64x_4(-16x_4^2 + x_1 + 77x_1x_2 + 3x_1x_2x_3)$ $\dot{x_9} = -x_9$
23	
$x_1^2{+}x_2^2{+}x_3^2{+}x_4^2{-}1{=}0 \wedge x_5{=}0$	$\dot{x_1} = x_1^2 - x_1(x_1^3 + x_2^3 + x_3^3 + x_4^3)$ $\dot{x_2} = x_2^2 - x_2(x_1^3 + x_2^3 + x_3^3 + x_4^3)$ $\dot{x_3} = x_3^2 - x_3(x_1^3 + x_2^3 + x_3^3 + x_4^3)$ $\dot{x_4} = x_4^2 - x_4(x_1^3 + x_2^3 + x_3^3 + x_4^3)$ $\dot{x_5} = -x_5$
24	

$(x_1x_2^2-12)(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2-1)=0 \wedge x_9=0$	$\dot{x_1} = -2(x_1x_2^2-12)x_5$ $\dot{x_2} = -2(x_1x_2^2-12)x_6$ $\dot{x_3} = -2(x_1x_2^2-12)x_7$ $\dot{x_4} = -2(x_1x_2^2-12)x_8$ $\dot{x_5} = (x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2-1)x_2^2+2x_1(x_1x_2^2-12)$ $\dot{x_6} = 2x_2(x_1x_2^2-12)+2x_1x_2(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2-1)$ $\dot{x_7} = 2(x_1x_2^2-12)x_3$ $\dot{x_8} = 2(x_1x_2^2-12)x_4$ $\dot{x_9} = x_9$
25	
$-\alpha-x_1^2+x_2^2-x_3=0 \wedge -x_1^2+3x_2^2+x_3=0$	$\dot{x_1} = 2x_3-2x_1^2$ $\dot{x_2} = -3x_1x_2$ $\dot{x_3} = 4x_1x_3-2x_1(2x_1^2-9x_2^2)$
26	
$J_1x_1x_4+J_2x_2x_5+J_3x_3x_6=0$	$\dot{x_1} = \frac{(J_2-J_3)x_2x_3-x_6X_2+x_5X_3}{J_1}$ $\dot{x_2} = \frac{(J_3-J_1)x_1x_3+x_6X_1-x_4X_3}{J_2}$ $\dot{x_3} = \frac{(J_1-J_2)x_1x_2-x_5X_1+x_4X_2}{J_3}$ $\dot{x_4} = x_3x_5-x_2x_6$ $\dot{x_5} = x_1x_6-x_3x_4$ $\dot{x_6} = x_2x_4-x_1x_5$
27	
$-\alpha-Jx_1x_6X_1+(x_1^2+x_2^2)x_3=0 \ \wedge \ 4x_1x_4+4x_2x_5+x_3x_6=0$	$\dot{x_1} = \frac{3x_2x_3}{4}$ $\dot{x_2} = \frac{1}{4}(Jx_6X_1-3x_1x_3)$ $\dot{x_3} = -Jx_5X_1$ $\dot{x_4} = x_3x_5-x_2x_6$ $\dot{x_5} = x_1x_6-x_3x_4$ $\dot{x_6} = x_2x_4-x_1x_5$
28	
$(x_1^2+x_2^2)x_3-Jx_1x_6X_1=0 \ \wedge \ 4x_1x_4+4x_2x_5+x_3x_6=0 \wedge \alpha(x_1^2+x_2^2)^3-2x_1^2=0$	$\dot{x_1} = \frac{3x_2x_3}{4}$ $\dot{x_2} = \frac{1}{4}(Jx_6X_1-3x_1x_3)$ $\dot{x_3} = -Jx_5X_1$ $\dot{x_4} = x_3x_5-x_2x_6$ $\dot{x_5} = x_1x_6-x_3x_4$ $\dot{x_6} = x_2x_4-x_1x_5$
29	
$x_4^2+x_5^2-1=0 \wedge x_6-x_4=0 \wedge x_4^2+x_5^2+1=0$	$\dot{x_4} = -x_5$ $\dot{x_5} = x_6$ $\dot{x_6} = -x_5$
30	
$x_1^2+x_2^2-1=0 \wedge x_3=0 \wedge x_4^2+x_5^2-1=0 \wedge x_6-x_4=0$	$\dot{x_1} = x_1(-x_1^2-x_2^2+1)-x_2$ $\dot{x_2} = x_1+x_2(-x_1^2-x_2^2+1)$ $\dot{x_3} = x_3$ $\dot{x_4} = -x_5$ $\dot{x_5} = x_6$ $\dot{x_6} = -x_5$
31	
$x_2^2x_1^4+x_2^4x_1^2-3x_2^2x_1^2+1=0 \wedge x_3=0$	$\dot{x_1} = (x_1-1)(x_1+1)$ $\dot{x_2} = (x_2-1)(x_2+1)$ $\dot{x_3} = -x_3$
32	

$$x_{13}=0 \quad \wedge \quad (x_6^2+x_7^2+x_8^2-1)^{146}+(x_{10}^4+2x_9x_{10}^3+6x_{10}^2+2x_9x_{10}+x_9^2-3)^{42}+(x_2^2x_1^4+x_2^4x_1^2-3x_2^2x_1^2+1)^{26}+(x_5^6-3x_3^2x_4^2x_5^2+x_3^2x_4^4+x_3^4x_4^2)^{14}+(x_{11}x_{12}+x_{12}-1)^2=0$$

$$\begin{aligned}
\dot{x_1} &= -292x_7(x_6^2+x_7^2+x_8^2-1)^{145}\\
\dot{x_2} &= -292x_8(x_6^2+x_7^2+x_8^2-1)^{145}\\
\dot{x_3} &= -42(2x_{10}^3+2x_{10}+2x_9)(x_{10}^4+2x_9x_{10}^3+6x_{10}^2+2x_9x_{10}+x_9^2-3)^{41}\\
\dot{x_4} &= -42(4x_{10}^3+6x_9x_{10}^2+12x_{10}+2x_9)\\
&\quad \times (x_{10}^4+2x_9x_{10}^3+6x_{10}^2+2x_9x_{10}+x_9^2-3)^{41}\\
\dot{x_5} &= -2x_{12}(x_{11}x_{12}+x_{12}-1)\\
\dot{x_6} &= -2(x_{11}+1)(x_{11}x_{12}+x_{12}-1)\\
\dot{x_7} &= 26(2x_1x_2^4+4x_1^3x_2^2-6x_1x_2^2)(x_2^2x_1^4+x_2^4x_1^2-3x_2^2x_1^2+1)^{25}\\
\dot{x_8} &= 26(2x_2x_1^4+4x_2^3x_1^2-6x_2x_1^2)(x_2^2x_1^4+x_2^4x_1^2-3x_2^2x_1^2+1)^{25}\\
\dot{x_9} &= 14(2x_3x_4^4+4x_3^3x_4^2-6x_3x_5^2x_4^2)(x_5^6-3x_3^2x_4^2x_5^2+x_3^2x_4^4+x_3^4x_4^2)^{13}\\
\dot{x_{10}} &= 14(2x_4x_3^4+4x_4^3x_3^2-6x_4x_5^2x_3^2)(x_5^6-3x_3^2x_4^2x_5^2+x_3^2x_4^4+x_3^4x_4^2)^{13}\\
\dot{x_{11}} &= 14(6x_5^5-6x_3^2x_4^2x_5)(x_5^6-3x_3^2x_4^2x_5^2+x_3^2x_4^4+x_3^4x_4^2)^{13}\\
\dot{x_{12}} &= 292x_6(x_6^2+x_7^2+x_8^2-1)^{145}\\
\dot{x_{13}} &= -x_{13}
\end{aligned}$$